Docket No.: H1658.0010/P010
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Keiichi Fukuda

Application No.: Not Yet Assigned

Filed: Concurrently Herewith

Art Unit: N/A

For: CONTENTS DATA TRANSMISSION/RECEPTION SYSTEM, CONTENTS DATA TRANSMITTER, CONTENTS DATA RECEIVER AND CONTENTS DATA TRANSMISSION/RECEPTION METHOD

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Japan	2003-313852	September 5, 2003

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: March 16, 2004

Respectfully submitted,

By _____

Mark J. Thronson
Registration No.: 33,082
DICKSTEIN SHAPIRO MORIN & OSHINSKY LLP
2101 L Street NW
Washington, DC 20037-1526
(202) 785-9700
Attorney for Applicant

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ９月 ５日

出 願 番 号
Application Number: 特願２００３－３１３８５２

[ST. 10/C]: [ＪＰ２００３－３１３８５２]

出 願 人
Applicant(s): 株式会社デノン

２００３年１２月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３１０５３６７

【書類名】　特許願
【整理番号】　DP3133
【提出日】　平成15年 9月 5日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明者】
　【住所又は居所】　福島県白河市字老久保山１番地１　株式会社デノン　白河ワークス内
　【氏名】　福田　圭一
【特許出願人】
　【識別番号】　301066006
　【氏名又は名称】　株式会社デノン
【代理人】
　【識別番号】　100074550
　【弁理士】
　【氏名又は名称】　林　實
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-279072
　【出願日】　平成14年 9月25日
【手数料の表示】
　【予納台帳番号】　155768
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
コンテンツデータを送信するコンテンツデータ送信装置とコンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータをキー情報を用いて暗号化し、前記キー情報を複数の信号路を介して前記コンテンツデータ受信装置に送信した後に暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信し、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信された前記キー情報を取得し、前記コンテンツデータ送信装置から複数の信号路を介して送信された前記暗号化したコンテンツデータを受信し、前記キー情報を用いて前記暗号化したコンテンツデータを復号することを特徴とするコンテンツデータ送受信システム。
【請求項２】
コンテンツデータを送信するコンテンツデータ送信装置とコンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータを暗号化するキー情報を生成するキー情報生成部と、前記コンテンツ再生部が再生したコンテンツデータを前記キー情報を用いて暗号化するコンテンツ暗号化部と、前記キー情報を複数の信号路を介してコンテンツデータ受信装置に送信すると共に前記暗号化されたコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する送信装置送受信部と、前記送信装置送受信部により前記キー情報を複数の信号路を介して送信した後に前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備え、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信されたデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータからキー情報を抽出するキー情報抽出部と、前記受信装置送受信部が受信したデータから前記暗号化したコンテンツデータを抽出し前記キー情報抽出部が抽出したキー情報を用いて暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力する出力部と、前記受信装置送受信部が受信したデータからキー情報を抽出し前記受信装置送受信部が受信した前記暗号化したコンテンツデータを復号する制御を行う受信装置制御部とを備えることを特徴とするコンテンツデータ送受信システム。
【請求項３】
コンテンツデータを送信するコンテンツデータ送信装置と当該コンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータの暗号化に用いる複数のキー情報を生成すると共に複数のキー情報の中からコンテンツデータの暗号化に用いるキー情報を選択するキー情報生成部と、前記コンテンツ再生部が再生したコンテンツデータを前記キー情報生成部が選択したキー情報を用いて暗号化するコンテンツ暗号化部と、前記複数のキー情報を複数の信号路及び前記暗号化されたコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共にコンテンツデータを送信する際に当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する送信装置送受信部と、該送信装置送受信部により前記複数のキー情報を複数の信号路を介して送信した後に前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共に当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備え、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信されたデータを受信する受信装置送受信部と、受信装置送受信部が受信したデータから複数のキー情報を抽出し記憶部に記憶すると共にキー情報に関する情報に基づいて記憶部に記憶した複数のキー情報からキー情報を選択するキー情報抽出部と、前記受信装置送受信部が受信したデータから前記暗号化したコンテンツデータを抽出し前記キー情報抽出部が選択したキー情報を用いて暗号化されたコ

ンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力する出力部と、前記受信装置送受信部が受信したデータから複数のキー情報を抽出して記憶部に記憶し前記受信装置送受信部が受信したキー情報に関する情報に基づいて記憶部に記憶した複数のキー情報からコンテンツデータの復号に用いるキー情報を選択し前記受信装置送受信部が受信した前記暗号化したコンテンツデータを復号する制御を行う受信装置制御部とを備えることを特徴とするコンテンツデータ送受信システム。

【請求項４】

請求項２及び請求項３記載のコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータ受信装置毎に割り当てられた受信装置ＩＤ情報を複数記憶する送信ＩＤ記憶部を有し、前記複数の受信装置ＩＤ情報のうちの１つの受信装置ＩＤ情報を選択すると共に前記コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報が送信されてきたことを確認する送信装置ＩＤ認証部を備え、前記送信装置制御部は、前記送信装置ＩＤ認証部が選択した受信装置ＩＤ情報を前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うと共に前記コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報を受信したときに前記キー情報及び前記暗号化したコンテンツデータを前記送信装置送受信部により複数の信号路を介してコンテンツデータ受信装置に送信する制御を行い、前記コンテンツデータ受信装置は、当該コンテンツデータ受信装置に割り当てられている受信装置ＩＤ情報を記憶する受信ＩＤ記憶部を有し、前記コンテンツデータ送信装置から送信された受信装置ＩＤ情報と前記受信ＩＤ記憶部が記憶する受信装置ＩＤ情報とを照合する受信装置ＩＤ認証部を備え、前記受信装置送受信部は、前記コンテンツデータ送信装置から送信された受信装置ＩＤ情報と前記受信ＩＤ記憶部に記憶した受信装置ＩＤ情報とが一致した場合に受信装置送受信部により信号路を介してコンテンツデータ送信装置に受信装置ＩＤ情報が一致した旨の情報を送信する制御を行うことを特徴とするコンテンツデータ送受信システム。

【請求項５】

コンテンツデータ受信装置にコンテンツデータを送信するコンテンツデータ送信装置において、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータを暗号化するためのキー情報を生成するキー情報生成部と、前記キー情報生成部が生成したキー情報を用いて前記コンテンツ再生部が再生したコンテンツデータを暗号化するコンテンツ暗号化部と、前記キー情報及び前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する送信装置送受信部と、前記キー情報を送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信した後に前記暗号化したコンテンツデータを送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備えることを特徴とするコンテンツデータ送信装置。

【請求項６】

コンテンツデータ受信装置にコンテンツデータを送信するコンテンツデータ送信装置において、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータの暗号化のために用いる複数のキー情報を生成すると共に前記複数のキー情報の中からコンテンツデータの暗号化に用いるキー情報を選択するキー情報生成部と、前記キー情報生成部が選択したキー情報を用いて前記コンテンツ再生部が再生したコンテンツデータを暗号化するコンテンツ暗号化部と、前記複数のキー情報及び前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共にコンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する送信装置送受信部と、前記複数のキー情報を送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信した後に前記暗号化したコンテンツデータを送信装置送受信部により複数の信号線を介して前記コンテンツデータ受信装置に送信すると共にコンテンツデータの暗号化に用いたキー情報に関する情報を送信装置送受信部により前記コンテンツデータ

受信装置に送信する制御を行う送信装置制御部とを備えることを特徴とするコンテンツデータ送信装置。

【請求項７】

請求項５及び請求項６記載のコンテンツデータ送信装置において、コンテンツデータ受信装置毎に割り当てられた受信装置ＩＤ情報を複数記憶する送信ＩＤ記憶部を有し、複数の受信装置ＩＤ情報のいずれか１つの受信装置ＩＤ情報を選択すると共に前記コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報が送信されてきたことを確認する送信装置ＩＤ認証部を備え、前記送信装置制御部は、前記受信装置ＩＤ情報を前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行う共に前記コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報を受信した後に前記キー情報及び前記暗号化したコンテンツデータを前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うことを特徴とするコンテンツデータ送信装置。

【請求項８】

コンテンツデータ送信装置が送信するコンテンツデータを受信するコンテンツデータ受信装置において、コンテンツデータ送信装置が複数の信号路を介して送信したデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータからキー情報を抽出するキー情報抽出部と、前記受信装置送受信部が受信したデータから暗号化したコンテンツデータを取得して前記キー情報抽出部が抽出したキー情報を用いて前記暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力するコンテンツ出力部と、前記コンテンツデータ送信装置が複数の信号路を介して送信したデータからキー情報を抽出し前記コンテンツデータ送信装置が複数の信号路を介して送信した暗号化したコンテンツデータを前記キー情報を用いて復号する制御を行う受信装置制御部とを備えることを特徴とするコンテンツデータ受信装置。

【請求項９】

コンテンツデータ送信装置が送信するコンテンツデータを受信するコンテンツデータ受信装置において、コンテンツデータ送信装置が信号線を介して送信したデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータから複数のキー情報を抽出し記憶部に記憶すると共に複数のキー情報の中から暗号化に用いたキー情報を選択するキー情報抽出部と、前記受信装置送受信部が受信したデータから暗号化したコンテンツデータを取得して前記キー情報抽出部が選択したキー情報を用いて前記暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力するコンテンツ出力部と、前記コンテンツデータ送信装置が複数の信号路を介して送信したデータから複数のキー情報を抽出し複数のキー情報の中からコンテンツデータの復号に用いるキー情報を選択し前記コンテンツデータ送信装置が複数の信号路を介して送信した暗号化したコンテンツデータを前記選択したキー情報を用いて復号する制御を行う受信装置制御部とを備えることを特徴とするコンテンツデータ受信装置。

【請求項１０】

請求項８及び請求項９記載のコンテンツデータ受信装置において、コンテンツデータ受信装置に割り当てられた受信装置ＩＤ情報を記憶する受信ＩＤ記憶部を有し、前記コンテンツデータ送信装置が送信した受信装置ＩＤ情報と前記受信ＩＤ記憶部が記憶している受信装置ＩＤ情報とを照合する受信装置ＩＤ認証部を備え、前記受信装置制御部は、コンテンツデータ送信装置が複数の信号路を介して送信した受信装置ＩＤ情報と前記受信ＩＤ記憶部に記憶された受信装置ＩＤ情報とが一致したときに受信装置ＩＤ情報が一致した旨の情報を受信装置送受信部により信号路を介して前記コンテンツデータ送信装置に送信する制御を行うことを特徴とするコンテンツデータ受信装置。

【請求項１１】

コンテンツデータ送信装置とコンテンツデータ受信装置との間でコンテンツデータの送受信を行うコンテンツデータ送受信方法において、コンテンツデータ受信装置毎に割り当てられた受信装置ＩＤ情報をコンテンツデータ送信装置から複数の信号路を介してコンテ

ンツデータ受信装置に送信する第１ステップと、コンテンツデータ送信装置から複数の信号路を介して送信された受信装置ＩＤ情報をコンテンツデータ受信装置が有する受信装置ＩＤ情報と照合し受信装置ＩＤ情報が一致した場合に受信装置ＩＤ情報が一致した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第２ステップと、コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報を受信した場合にコンテンツデータを暗号化したキー情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第３ステップと、コンテンツデータ送信装置から送信さたれデータからキー情報を抽出したときにキー情報を受信した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第４ステップと、コンテンツデータ受信装置からキー情報を受信した旨の情報を受信したとき暗号化コンテンツデータをコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第５ステップとを有することを特徴とするコンテンツデータ送受信方法。

【請求項１２】

コンテンツデータ送信装置とコンテンツデータ受信装置との間でコンテンツデータの送受信を行うコンテンツデータ送受信方法において、コンテンツデータ受信装置毎に割り当てられた受信装置ＩＤ情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第１ステップと、コンテンツデータ送信装置から複数の信号路を介して送信された受信装置ＩＤ情報をコンテンツデータ受信装置が有する受信装置ＩＤ情報と照合し受信装置ＩＤ情報が一致した場合に受信装置ＩＤ情報が一致した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第２ステップと、コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報を受信した場合にコンテンツデータを暗号化するための複数のキー情報を生成しコンテンツデータ送信装置からコンテンツデータ受信装置に送信する第３ステップと、コンテンツデータ送信装置から送信さたれデータから複数のキー情報を抽出したときにキー情報を受信した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第４ステップと、コンテンツデータ受信装置からキー情報を受信した旨の情報を受信したとき前記複数のキー情報から暗号化に用いるキー情報を選択し当該選択したキー情報を用いてコンテンツデータを暗号化し暗号化したコンテツデータと当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第５ステップと、コンテンツデータ送信装置から送信されてきたキー情報に関する情報に基づいて複数のキー情報の中からコンテンツデータの暗号化に用いたキー情報を選択しコンテンツデータ送信装置から送信されてきた暗号化されたコンテンツデータを復号する第６ステップとを有することを特徴とするコンテンツデータ送受信方法。

【書類名】明細書
【発明の名称】コンテンツデータ送受信システム、コンテンツデータ送信装置、コンテンツデータ受信装置及びコンテンツデータ送受信方法
【技術分野】
【０００１】
本発明は、複数の装置間でオーディオデータやビデオデータ等のコンテンツデータを送受信するコンテンツデータ送受信システム、コンテンツデータ送信装置、コンテンツデータ受信装置およびコンテンツデータ送信方法に関する。
【背景技術】
【０００２】
大容量のデータを記録することができる記録媒体としてデジタル・バーサタイル・ディスク（Digital Versatile Disc、以下「ＤＶＤ」という。）がある。ＤＶＤには、ビデオデータとオーディオデータとを記録したＤＶＤ－ＶＩＤＥＯや、高音質のオーディオデータを記録したＤＶＤ－ＡＵＤＩＯがある。これらのＤＶＤを再生する光ディスク再生装置は、ＤＶＤに記録されているデジタルデータを再生し、オーディオデータをアナログ信号としてアナログ出力したり、２チャンネルのデジタルデータとしてデジタル出力することができる。
【０００３】
ＤＶＤには、レフト（Ｌ）チャンネル、ライト（Ｒ）チャンネル、サラウンドレフト（ＳＬ）チャンネル、サラウンドライト（ＳＲ）チャンネル、センター（Ｃ）チャンネルなどの複数のチャンネル（マルチチャンネル）のオーディオデータが記録されている場合がある。光ディスク再生装置は、ＤＶＤに記録されたマルチチャンネルのオーディオデータをデジタル出力する場合、マルチチャンネルのオーディオデータを２チャンネルのデジタルデータにダウンミックスし、ダウンミックスしたデータをＩＥＣ（International Electrotechanical Commission）９５８のデータフォーマットに準拠したデジタルデータとして出力する。
【０００４】
光ディスク再生装置からアナログ出力されるオーディオデータは、信号伝送中にノイズが重畳することにより音質が劣化することがある。光ディスク再生装置からデジタル出力されるオーディオデータは、アナログ出力のオーディオデータに比べ、信号伝送中のノイズの重畳による音質劣化がない。
【０００５】
光ディスク再生装置からデジタル出力されるオーディオデータは、ＤＶＤに記録されているマルチチャンネルのオーディオデータを２チャンネルのオーディオデータに変換して出力しており、光ディスク再生装置から出力されたオーディオデータを増幅してスピーカ等に出力する増幅装置（例えば、オーディオビジュアル（Audio Visual、以下「ＡＶ」といぅ。）アンプ）は、光ディスク再生装置からデジタル出力された２チャンネルのオーディオデータを受け取り、マルチチャンネルのオーディオデータに変換し出力する。
【０００６】
増幅装置において、入力した２チャンネルのオーディオデータをマルチチャンネルのオーディオデータに変換する処理は、増幅装置に搭載された変換手段による演算により行われる。この演算処理は、その処理方法や演算に用いられるパラメータが変換手段（例えば、デジタル・シグナル・プロセッサ（Digital Signal Processor、以下「ＤＳＰ」という。））の製造者毎に異なるため、入力した２チャンネルのオーディオデータをＤＶＤに記録されている元のマルチチャンネルのオーディオデータに忠実に変換することができない。言い換えれば、２チャンネルのオーディオデータをマルチチャンネルのオーディオデータに変換することにより、光ディスクに記録されたマルチチャンネルのオーディオデータよりも音質が劣化したオーディオデータが増幅装置から出力されることになる。
【０００７】
このため、マルチチャンネルのデジタルデータに上述の変換処理を行わずに、光ディス

ク再生装置により再生されたオーディオデータをマルチチャンネルのままデジタル出力し、デジタルデータの受け側である増幅装置が、マルチチャンネルのデジタルオーディオデータをアナログオーディオ信号に変換して出力することにより、光ディスクに記録された高音質のオーディオデータを忠実に再生したいという要望が高まっている。

【０００８】

しかし、光ディスク再生装置からマルチチャンネルのデジタルオーディオデータを出力するようにした場合、このデジタルオーディオデータを記録媒体に複製記録することが可能になる。このデジタルオーディオデータの不正複製を防止するため、特許文献１に開示されているデータ伝送システムや、特許文献２に開示されているコンテンツ配布システムのような、２台の装置間で暗号化されたコンテンツデータを送受信する技術を用いることが考えられる。

【０００９】

特許文献１に開示されているデータ伝送システムは、クライアントコンピュータが暗号キーと復号キーを生成し、サーバコンピュータに暗号キーと画像データ転送要求を送り、サーバコンピュータは、暗号キーにより画像データを暗号化し、暗号化した画像データをクライアントコンピュータに送信し、クライアントコンピュータは、保持している復号キーを用いて暗号化された画像データを復号化する。

【００１０】

特許文献２に開示されているコンテンツ配布システムは、クライアントからサーバに、ユーザＩＤ、認証ＩＤ及びコンテンツデータのダウンロード要求が送信され、サーバのコンテンツサーバにユーザＩＤとコンテンツデータが登録されており、且つ、サーバが保持している認証ＩＤとクライアントから送信された認証ＩＤが同一である場合、サーバは、暗号化コンテンツを解読する解読鍵を生成し、暗号化コンテンツデータと解読鍵とをクライアントに送信する。ライアントは、サーバから送信された解読鍵を用いて暗号化コンテンツデータを解読し、コンテンツデータを再生する。

【００１１】

【特許文献１】特開平１１－２８９３２３号公報

【特許文献２】特開２０００－２４２６０４号公報

【発明の開示】

【発明が解決しようとする課題】

【００１２】

前述した特許文献１に開示されているデータ伝送システムや特許文献２に開示されているコンテンツ配布システムでは、コンテンツデータを１つのキー情報を用いて暗号化し、装置間を接続する単一の信号線を用いて、暗号化したコンテンツデータと暗号化したコンテンツデータの暗号を解読するための暗号解除情報（キー情報）を送信する。

【００１３】

このようなシステムでは、コンテンツデータを１つのキー情報によってのみ暗号化し、この暗号解除情報（キー情報）を一塊りの情報として単一の信号線を介してコンテンツデータ送信装置からコンテンツデータ受信装置に送るため、２台の装置間で伝送されているデータの中からその情報を取り出し、その暗号解除情報を用いて暗号化コンテンツデータを復号し、元の高品質のコンテンツデータを得ることができるという問題がある。

【００１４】

本発明は、装置間で送受信する暗号化されたコンテンツデータを復号するための暗号解除情報を抽出し容易に解読することができないコンテンツデータ送受信システム、コンテンツデータ送信装置、コンテンツデータ受信装置及びコンテンツデータ送受信方法を提供することを目的とする。

【課題を解決するための手段】

【００１５】

上記課題を解決するために、本願の請求項１の発明は、コンテンツデータを送信するコンテンツデータ送信装置とコンテンツデータを受信するコンテンツデータ受信装置とを備

えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータをキー情報を用いて暗号化し、前記キー情報を複数の信号路を介して前記コンテンツデータ受信装置に送信した後に暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信し、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信された前記キー情報を取得し、前記コンテンツデータ送信装置から複数の信号路を介して送信された前記暗号化したコンテンツデータを受信し、前記キー情報を用いて前記暗号化したコンテンツデータを復号することを特徴とする。

【００１６】

本願の請求項２の発明は、コンテンツデータを送信するコンテンツデータ送信装置とコンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータを暗号化するキー情報を生成するキー情報生成部と、前記コンテンツ再生部が再生したコンテンツデータを前記キー情報を用いて暗号化するコンテンツ暗号化部と、前記キー情報を複数の信号路を介してコンテンツデータ受信装置に送信すると共に前記暗号化されたコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する送信装置送受信部と、前記送信装置送受信部により前記キー情報を複数の信号路を介して送信した後に前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備え、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信されたデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータからキー情報を抽出するキー情報抽出部と、前記受信装置送受信部が受信したデータから前記暗号化したコンテンツデータを抽出し前記キー情報抽出部が抽出したキー情報を用いて暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力する出力部と、前記受信装置送受信部が受信したデータからキー情報を抽出し前記受信装置送受信部が受信した前記暗号化したコンテンツデータを復号する制御を行う受信装置制御部とを備えることを特徴とする。

【００１７】

本願の請求項３の発明は、コンテンツデータを送信するコンテンツデータ送信装置と当該コンテンツデータを受信するコンテンツデータ受信装置とを備えたコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータの暗号化に用いる複数のキー情報を生成すると共に複数のキー情報の中からコンテンツデータの暗号化に用いるキー情報を選択するキー情報生成部と、前記コンテンツ再生部が再生したコンテンツデータを前記キー情報生成部が選択したキー情報を用いて暗号化するコンテンツ暗号化部と、前記複数のキー情報を複数の信号路及び前記暗号化されたコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共にコンテンツデータを送信する際に当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する送信装置送受信部と、該送信装置送受信部により前記複数のキー情報を複数の信号路を介して送信した後に前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共に当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備え、前記コンテンツデータ受信装置は、コンテンツデータ送信装置から複数の信号路を介して送信されたデータを受信する受信装置送受信部と、受信装置送受信部が受信したデータから複数のキー情報を抽出し記憶部に記憶すると共にキー情報に関する情報に基づいて記憶部に記憶した複数のキー情報からキー情報を選択するキー情報抽出部と、前記受信装置送受信部が受信したデータから前記暗号化したコンテンツデータを抽出し前記キー情報抽出部が選択したキー情報を用いて暗号化されたコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力する出力部と、前記受信装置送受信部が受信したデータから複数のキー情報を抽出して記憶部に記憶し前記受信装置送受信部が受

信したキー情報に関する情報に基づいて記憶部に記憶した複数のキー情報からコンテンツデータの復号に用いるキー情報を選択し前記受信装置送受信部が受信した前記暗号化したコンテンツデータを復号する制御を行う受信装置制御部とを備えることを特徴とする。

【００１８】

本願の請求項４の発明は、請求項２及び請求項３記載のコンテンツデータ送受信システムにおいて、前記コンテンツデータ送信装置は、コンテンツデータ受信装置毎に割り当てられた受信装置ＩＤ情報を複数記憶する送信ＩＤ記憶部を有し、前記複数の受信装置ＩＤ情報のうちの１つの受信装置ＩＤ情報を選択すると共に前記コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報が送信されてきたことを確認する送信装置ＩＤ認証部を備え、前記送信装置制御部は、前記送信装置ＩＤ認証部が選択した受信装置ＩＤ情報を前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うと共に前記コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報を受信したときに前記キー情報及び前記暗号化したコンテンツデータを前記送信装置送受信部により複数の信号路を介してコンテンツデータ受信装置に送信する制御を行い、前記コンテンツデータ受信装置は、当該コンテンツデータ受信装置に割り当てられている受信装置ＩＤ情報を記憶する受信ＩＤ記憶部を有し、前記コンテンツデータ送信装置から送信された受信装置ＩＤ情報と前記受信ＩＤ記憶部が記憶する受信装置ＩＤ情報とを照合する受信装置ＩＤ認証部を備え、前記受信装置送受信部は、前記コンテンツデータ送信装置から送信された受信装置ＩＤ情報と前記受信ＩＤ記憶部に記憶した受信装置ＩＤ情報とが一致した場合に受信装置送受信部により信号路を介してコンテンツデータ送信装置に受信装置ＩＤ情報が一致した旨の情報を送信する制御を行うことを特徴とする。

【００１９】

本願の請求項５の発明は、コンテンツデータ受信装置にコンテンツデータを送信するコンテンツデータ送信装置において、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータを暗号化するためのキー情報を生成するキー情報生成部と、前記キー情報生成部が生成したキー情報を用いて前記コンテンツ再生部が再生したコンテンツデータを暗号化するコンテンツ暗号化部と、前記キー情報及び前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する送信装置送受信部と、前記キー情報を送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信した後に前記暗号化したコンテンツデータを送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備えることを特徴とする。

【００２０】

本願の請求項６の発明は、コンテンツデータ受信装置にコンテンツデータを送信するコンテンツデータ送信装置において、コンテンツデータを再生するコンテンツ再生部と、コンテンツデータの暗号化のために用いる複数のキー情報を生成すると共に前記複数のキー情報の中からコンテンツデータの暗号化に用いるキー情報を選択するキー情報生成部と、前記キー情報生成部が選択したキー情報を用いて前記コンテンツ再生部が再生したコンテンツデータを暗号化するコンテンツ暗号化部と、前記複数のキー情報及び前記暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信すると共にコンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ受信装置に送信する送信装置送受信部と、前記複数のキー情報を送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信した後に前記暗号化したコンテンツデータを送信装置送受信部により複数の信号線を介して前記コンテンツデータ受信装置に送信すると共にコンテンツデータの暗号化に用いたキー情報に関する情報を送信装置送受信部により前記コンテンツデータ受信装置に送信する制御を行う送信装置制御部とを備えることを特徴とする。

【００２１】

本願の請求項７の発明は、請求項５及び請求項６記載のコンテンツデータ送信装置において、コンテンツデータ受信装置毎に割り当てられた受信装置ＩＤ情報を複数記憶する送

信ＩＤ記憶部を有し、複数の受信装置ＩＤ情報のいずれか１つの受信装置ＩＤ情報を選択すると共に前記コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報が送信されてきたことを確認する送信装置ＩＤ認証部を備え、前記送信装置制御部は、前記受信装置ＩＤ情報を前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行う共に前記コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報を受信した後に前記キー情報及び前記暗号化したコンテンツデータを前記送信装置送受信部により複数の信号路を介して前記コンテンツデータ受信装置に送信する制御を行うことを特徴とする。

【００２２】

本願の請求項８の発明は、コンテンツデータ送信装置が送信するコンテンツデータを受信するコンテンツデータ受信装置において、コンテンツデータ送信装置が複数の信号路を介して送信したデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータからキー情報を抽出するキー情報抽出部と、前記受信装置送受信部が受信したデータから暗号化したコンテンツデータを取得して前記キー情報抽出部が抽出したキー情報を用いて前記暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力するコンテンツ出力部と、前記コンテンツデータ送信装置が複数の信号路を介して送信したデータからキー情報を抽出し前記コンテンツデータ送信装置が複数の信号路を介して送信した暗号化したコンテンツデータを前記キー情報を用いて復号する制御を行う受信装置制御部とを備えることを特徴とする。

【００２３】

本願の請求項９の発明は、コンテンツデータ送信装置が送信するコンテンツデータを受信するコンテンツデータ受信装置において、コンテンツデータ送信装置が信号線を介して送信したデータを受信する受信装置送受信部と、前記受信装置送受信部が受信したデータから複数のキー情報を抽出し記憶部に記憶すると共に複数のキー情報の中から暗号化に用いたキー情報を選択するキー情報抽出部と、前記受信装置送受信部が受信したデータから暗号化したコンテンツデータを取得して前記キー情報抽出部が選択したキー情報を用いて前記暗号化したコンテンツデータを復号するコンテンツ復号化部と、前記コンテンツ復号化部が復号したコンテンツデータを出力するコンテンツ出力部と、前記コンテンツデータ送信装置が複数の信号路を介して送信したデータから複数のキー情報を抽出し複数のキー情報の中からコンテンツデータの復号に用いるキー情報を選択し前記コンテンツデータ送信装置が複数の信号路を介して送信した暗号化したコンテンツデータを前記選択したキー情報を用いて復号する制御を行う受信装置制御部とを備えることを特徴とする。

【００２４】

本願の請求項１０の発明は、請求項８及び請求項９記載のコンテンツデータ受信装置において、コンテンツデータ受信装置に割り当てられた受信装置ＩＤ情報を記憶する受信ＩＤ記憶部を有し、前記コンテンツデータ送信装置が送信した受信装置ＩＤ情報と前記受信ＩＤ記憶部が記憶している受信装置ＩＤ情報とを照合する受信装置ＩＤ認証部を備え、前記受信装置制御部は、コンテンツデータ送信装置が複数の信号路を介して送信した受信装置ＩＤ情報と前記受信ＩＤ記憶部に記憶された受信装置ＩＤ情報とが一致したときに受信装置ＩＤ情報が一致した旨の情報を受信装置送受信部により信号路を介して前記コンテンツデータ送信装置に送信する制御を行うことを特徴とする。

【００２５】

本願の請求項１１の発明は、コンテンツデータ送信装置とコンテンツデータ受信装置との間でコンテンツデータの送受信を行うコンテンツデータ送受信方法において、コンテンツデータ受信装置毎に割り当てられた受信装置ＩＤ情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第１ステップと、コンテンツデータ送信装置から複数の信号路を介して送信された受信装置ＩＤ情報をコンテンツデータ受信装置が有する受信装置ＩＤ情報と照合し受信装置ＩＤ情報が一致した場合に受信装置ＩＤ情報が一致した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第２ステップと、コンテンツデータ受信装置から受信装置Ｉ

Ｄ情報が一致した旨の情報を受信した場合にコンテンツデータを暗号化したキー情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第３ステップと、コンテンツデータ送信装置から送信されたデータからキー情報を抽出したときにキー情報を受信した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第４ステップと、コンテンツデータ受信装置からキー情報を受信した旨の情報を受信したとき暗号化コンテンツデータをコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第５ステップとを有することを特徴とする。

【００２６】

本願の請求項１２の発明は、コンテンツデータ送信装置とコンテンツデータ受信装置との間でコンテンツデータの送受信を行うコンテンツデータ送受信方法において、コンテンツデータ受信装置毎に割り当てられた受信装置ＩＤ情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第１ステップと、コンテンツデータ送信装置から複数の信号路を介して送信された受信装置ＩＤ情報をコンテンツデータ受信装置が有する受信装置ＩＤ情報と照合し受信装置ＩＤ情報が一致した場合に受信装置ＩＤ情報が一致した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第２ステップと、コンテンツデータ受信装置から受信装置ＩＤ情報が一致した旨の情報を受信した場合にコンテンツデータを暗号化するための複数のキー情報を生成しコンテンツデータ送信装置からコンテンツデータ受信装置に送信する第３ステップと、コンテンツデータ送信装置から送信されたデータから複数のキー情報を抽出したときにキー情報を受信した旨の情報をコンテンツデータ受信装置から信号路を介してコンテンツデータ送信装置に送信する第４ステップと、コンテンツデータ受信装置からキー情報を受信した旨の情報を受信したとき前記複数のキー情報から暗号化に用いるキー情報を選択し当該選択したキー情報を用いてコンテンツデータを暗号化し暗号化したコンテツデータと当該コンテンツデータの暗号化に用いたキー情報に関する情報をコンテンツデータ送信装置から複数の信号路を介してコンテンツデータ受信装置に送信する第５ステップと、コンテンツデータ送信装置から送信されてきたキー情報に関する情報に基づいて複数のキー情報の中からコンテンツデータの暗号化に用いたキー情報を選択しコンテンツデータ送信装置から送信されてきた暗号化されたコンテンツデータを復号する第６ステップとを有することを特徴とする。

【発明の効果】

【００２７】

本発明によれば、装置間で送受信する暗号化されたコンテンツデータを復号するための暗号解除情報を抽出し容易に解読することができないコンテンツデータ送受信システム、コンテンツデータ送信装置、コンテンツデータ受信装置及びコンテンツデータ送受信方法を提供することができる。

【発明を実施するための最良の形態】

【００２８】

図１は、本発明のコンテンツデータ送受信システムの一実施例を示す概略構成図である。

図１において、コンテンツデータ送受信システム１０は、コンテンツデータ送信装置２０とコンテンツデータ受信装置３０とを備える。コンテンツデータ送受信システム１０は、コンテンツデータ送信装置２０がキー情報を用いてコンテンツデータを暗号化し、キー情報と暗号化したコンテンツデータ（暗号化コンテンツデータ）をコンテンツデータ受信装置３０に送信し、コンテンツデータ受信装置３０がコンテンツデータ送信装置２０から送信されたキー情報と暗号化コンテンツデータとを受信し、キー情報を用いて暗号化コンテンツデータの暗号を解除するシステムである。

【００２９】

コンテンツデータ送信装置２０は、例えば、ＤＶＤ等の記録媒体に記録されているビデオデータ及びオーディオデータを再生して出力するＤＶＤ－Ｖｉｄｅｏプレーヤなどの再

生装置である。本実施例において、コンテンツデータ送信装置２０は、再生装置として説明するが、ネットワークを介して伝送されるコンテンツデータを受信し、受信したコンテンツデータを出力する装置などであってもよい。

【００３０】

コンテンツデータ受信装置３０は、例えば、ＤＶＤ－Ｖｉｄｅｏプレーヤから出力されたビデオデータ及びオーディオデータを受信し、ビテオデータをビデオ信号に変換してモニタ等の映像装置に出力し、オーディオデータをオーディオ信号に変換して増幅しスピーカに出力するＡＶ（Audio Visual）アンプなどの増幅装置である。本実施例において、コンテンツデータ受信装置３０は、増幅装置として説明するが、コンテンツデータ送信装置２０から送信されたコンテンツデータを受信し、コンテンツデータを編集して出力する装置などであってもよい。

【００３１】

コンテンツデータ送信装置２０とコンテンツデータ受信装置３０とは、ビデオデータを伝送するビデオデータ伝送路と、オーディオデータを伝送するオーディオデータ伝送路とにより接続されている。本実施例においては、ビデオデータ伝送路の説明を省略し、オーディオデータ伝送路についてのみ説明する。

【００３２】

本実施例においては、図１に示すコンテンツデータ送信装置２０とコンテンツデータ受信装置３０との間のオーディオデータ伝送路は、７本の信号線で接続されているものとする。７本の信号線うちの６本の信号線は、コンテンツデータ送信装置２０からコンテンツデータ受信装置３０にデータ（後述する接続確認データ、機器認証データ、キー情報送信データ及びコンテンツ送信データ）を送信する第１データ線～第６データ線であり、７本の信号線のうち残りの１本の信号線は、コンテンツデータ受信装置３０からコンテンツデータ送信装置２０にデータ（後述する接続確認応答データ、機器認証応答データ、キー情報受信データ及びコンテンツ受信データ）を送信する応答線である。このようなオーディオデータ伝送路は、複数の信号線を伝送するデータとしてデジタル・オーディオ・インターフェースに準拠したフォーマットを利用することができる。なお、本実施例では、コンテンツデータ送信装置とコンテンツデータ受信装置との間のデータ伝送を信号線により行うものとして説明するが、それに限定されず、無線によりデータ伝送を行ってもよい。

【００３３】

コンテンツデータ送信装置２０は、コンテンツ再生部２１、コンテンツ暗号化部２２、キー情報生成部２３、送信装置ＩＤ認証部２４、送信装置送受信部２５、送信装置制御部２６を備える。

【００３４】

コンテンツ再生部２１は、記録媒体に記録されたコンテンツデータ（オーディオデータ）を再生してコンテンツ暗号化部２２に出力する。

【００３５】

コンテンツ暗号化部２２は、キー情報生成部２３により生成されたキー情報を用いてコンテンツ再生部２１が再生したコンテンツデータを暗号化する。コンテンツ暗号化部２２における暗号化方法は、特に限定されずどのような方法でもよい。

【００３６】

キー情報生成部２３は、コンテンツデータを暗号化するキー情報を生成し、コンテンツ暗号化部２２に出力する。キー情報は、例えば、複数ビットのデータ列からなる情報であり、キー情報の生成方法は特に限定されずどのような方法でもよい。

【００３７】

また、キー情報生成部２３は、生成したキー情報をコンテンツデータ受信装置３０に送信する場合に、生成したキー情報を暗号化して送信装置送受信部２５に出力する。

【００３８】

キー情報生成部２３におけるキー情報の暗号化は、予め定められた方法により行われる。後述するコンテンツデータ受信装置３０のキー情報抽出部３３は、コンテンツデータ送

信装置２０のキー情報生成部２３が行ったキー情報の暗号化を解除する復号処理機能を備え、キー情報生成部２３が暗号化したキー情報は、後述するキー情報抽出部３３により復号が可能である。本実施例では、キー情報生成部２３がキー情報を暗号化してコンテンツデータ受信装置３０に送信するが、暗号化せずにキー情報をコンテンツデータ受信装置３０に送信するようにしてもよい。

【００３９】

送信装置ＩＤ認証部２４は、コンテンツデータ受信装置毎に固有に割り当てられた複数の受信装置ＩＤ情報を記憶する送信ＩＤ記憶部２４ａを備える。送信装置ＩＤ認証部２４は、後述する機器認証のときに、送信ＩＤ記憶部２４ａに記憶された複数の受信装置ＩＤ情報の中から１つを選択し、受信ＩＤ情報を暗号化して送信装置送受信部２５に出力する。

【００４０】

送信装置ＩＤ認証部２４における受信装置ＩＤ情報の暗号化方法は、特に限定されずどのような方法でもよい。後述するコンテンツデータ受信装置３０の受信装置ＩＤ認証部３２は、送信装置ＩＤ認証部２４による受信装置ＩＤ情報の暗号化を解除する復号処理機能を備え、当該送信装置ＩＤ認証部２４が暗号化した受信装置ＩＤ情報は、後述する受信装置ＩＤ認証部３２により復号が可能である。本実施例では、送信装置ＩＤ認証部２４が受信装置ＩＤ情報を暗号化してコンテンツデータ受信装置３０に送信するが、暗号化せずに受信装置ＩＤ情報をコンテンツデータ受信装置３０に送信するようにしてもよい。

【００４１】

また、送信装置ＩＤ認証部２４は、送信装置送受信部２５が受信したコンテンツデータ受信装置３０から送信されてきた受信装置ＩＤ情報と送信ＩＤ記憶部２４ａに記憶している複数の受信装置ＩＤ情報とを照合し、照合した結果を送信装置制御部２６に通知する。

【００４２】

送信装置送受信部２５は、送信装置制御部２６の制御により、コンテンツデータ送信装置２０とコンテンツデータ受信装置３０との間の接続確認を行うためのデータ（接続確認データ及び接続確認応答データ）の送受信、機器認証を行うためのデータ（機器認証データ及び機器認証応答データ）の送受信、暗号化コンテンツデータの暗号を解除するキー情報に関するデータ（キー情報送信データ及びキー情報受信データ）の送受信、暗号化コンテンツデータの送受信に関するデータ（コンテンツ送信データ及びコンテンツ受信データ）の送受信を行う。

【００４３】

後述するが、機器認証データ、キー情報送信データ及びコンテンツ送信データは、それぞれ複数のデータ列からなる。送信装置送受信部２５は、送信装置制御部２６の制御により、キー情報生成部２３から出力される暗号化されたキー情報、送信装置ＩＤ認証部２４から出力される暗号化された受信装置ＩＤ情報、コンテンツ暗号化部から出力される暗号化されたコンテンツデータをそれぞれ分割し、分割したそれぞれのデータを機器認証データ、キー情報送信データ、コンテンツ送信データが有する複数のデータ列にそれぞれ格納する処理を行い、それぞれのデータをコンテンツデータ受信装置３０に送信する。

【００４４】

送信装置制御部２６は、コンテンツデータ送信装置２０を総合的に制御する。送信装置制御部２６は、操作部（図示せず）により再生開始の指示があると、コンテンツ再生部２１における記録媒体に記録されているコンテンツデータの再生の制御を行う。

【００４５】

送信装置制御部２６は、コンテンツデータ送信装置２０とコンテンツデータ受信装置３０との間の接続確認及び機器認証が終了すると、キー情報生成部２３においてコンテンツデータを暗号化するためのキー情報を生成する制御を行う。また、送信装置制御部２６は、生成したキー情報を暗号化する制御を行う。

【００４６】

送信装置制御部２６は、コンテンツ暗号化部２２において、コンテンツ再生部２１が再

生したコンテンツデータをキー情報生成部２３が生成したキー情報を用いて暗号化する制御を行う。

【００４７】

送信装置制御部２６は、送信装置送受信部２５における接続確認データ及び接続確認応答データの送受信、機器認証データ及び機器認証応答データの送受信、キー情報送信データ及びキー情報受信データの送受信、コンテンツ送信データ及びコンテンツ受信データの送受信の制御を行う。

【００４８】

送信装置制御部２６は、コンテンツ暗号化部２２が暗号化した暗号化コンテンツデータをコンテンツデータ受信装置３０に送信する前に、コンテンツデータ送信装置２０とコンテンツデータ受信装置３０とが接続されていることを確認する接続確認データを、一本又は複数本のデータ線を介してコンテンツデータ受信装置２０に送信する制御を行う。送信装置制御部２６は、コンテンツデータ受信装置３０から応答線を介して送信された接続確認応答データを受信すると、コンテンツデータ送信装置３０とコンテンツデータ受信装置２０との間が接続されていると判断する。

【００４９】

送信装置制御部２６は、コンテンツデータ送信装置２０とコンタンツデータ受信装置３０との間の接続確認が終了すると、送信装置ＩＤ認証部２４の送信ＩＤ記憶部２４ａに記憶されている複数の受信装置ＩＤ情報の中からコンテンツデータ受信装置２０に対応する１つの受信装置ＩＤ情報を抽出し、当該受信装置ＩＤ情報を暗号化した受信装置ＩＤ情報を分割し、分割したそれぞれのデータを複数のデータ列からなる機器認証データにそれぞれ格納し、機器認証データを送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する制御を行う。

【００５０】

送信装置制御部２６は、送信装置ＩＤ認証部２４がコンテンツデータ受信装置３０から応答線を介して送信されてきた機器認証応答データに格納されている受信装置ＩＤ情報と、送信ＩＤ記憶部２４ａに記憶してある受信装置ＩＤ情報とを照合した結果、両方の受信装置ＩＤ情報が一致している場合、機器認証を終了する。

【００５１】

送信装置制御部２６は、コンテンツデータ受信装置３０から送信された受信装置ＩＤ情報と送信ＩＤ記憶部２４ａに記憶してある受信装置ＩＤ情報とが一致していない場合、送信装置ＩＤ認証部２４に、送信ＩＤ記憶部２４ａに記憶されている複数の受信装置ＩＤ情報の中から、既に抽出した受信装置ＩＤ情報以外の受信装置ＩＤ情報を抽出させて暗号化させる制御を行う。そして、送信装置ＩＤ認証部２４が暗号化した受信装置ＩＤ情報を分割し、分割したデータを複数のデータ列からなる機器認証データにそれぞれ格納し、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する制御を行う。

【００５２】

送信装置制御部２６は、機器認証が終了すると、キー情報生成部２３が生成し暗号化したキー情報を分割し、分割したデータを複数のデータ列からなるキー情報送信データにそれぞれ格納し、キー情報送信データを送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する制御を行う。

【００５３】

送信装置制御部２６は、コンテンツデータ受信装置３０から応答線を介して送信されてきたキー情報受信データに格納されている情報が、コンテンツデータ受信装置３０においてキー情報を取得した旨の情報であるか否かの確認を行う。送信装置制御部２６は、キー情報受信データに格納されている情報がキー情報を取得していない旨の情報の場合、再度キー情報送信データを送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する制御を行う。

【００５４】

送信装置制御部２６は、コンテンツデータ受信装置３０がキー情報を取得したことを確認すると、コンテンツ暗号化部２２により暗号化された暗号化データを分割し、分割したデータを複数のデータ列からなるコンテンツ送信データにそれぞれ格納し、コンテンツ送信データを送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する制御を行う。

【００５５】

コンテンツデータ受信装置３０は、受信装置送受信部３１、受信装置ＩＤ認証部３２、キー情報抽出部３３、コンテンツ復号化部３４、出力部３５、受信装置制御部３６を備える。

【００５６】

受信装置送受信部３６は、コンテンツデータ送信装置２０とコンテンツデータ受信装置３０との間の接続確認のためのデータ（接続確認データ及び接続確認応答データ）の送受信、機器認証を行うためのデータ（機器認証データ及び機器認証応答データ）の送受信、暗号化コンテンツデータの暗号を解除するためのキー情報に関するデータ（キー情報送信データ及びキー情報受信データ）の送受信、暗号化コンテンツデータの送受信に関するデータ（コンテンツ送信データ及びコンテンツ受信データ）の送受信を行う。

【００５７】

後述するが、機器認証応答データ、キー情報受信データ及びコンテンツ受信データは、それぞれ複数のデータ列からなる。受信装置送受信部３１は、受信装置制御部３６の制御により、キー情報抽出部３３から送信装置送受信部２５を介して出力されたキー情報を取得したか否かを示すデータ、送信装置ＩＤ認証部３２から送信装置送受信部２５を介して出力される受信装置ＩＤ情報が一致したか否かを示すデータ、コンテンツ暗号化部２２から送信装置送受信部２５を介して出力された暗号化コンテンツデータを取得したか否かを示すデータをそれぞれ分割し、分割したそれぞれのデータを機器認証応答データ、キー情報受信データ、コンテンツ受信データが有する複数のデータ列にそれぞれ格納する処理を行い、それぞれのデータをコンテンツデータ送信装置２０に送信する。

【００５８】

受信装置ＩＤ認証部３２は、当該コンテンツデータ受信装置３０に固有に割り当てられた受信装置ＩＤ情報を記憶する受信ＩＤ記憶部３２ａを備える。受信装置ＩＤ認証部３２は、機器認証のときに、コンテンツデータ送信装置２０から送信されてきた受信装置ＩＤ情報と、受信ＩＤ記憶部３２ａに記憶されている受信装置ＩＤ情報とを照合し、照合した結果を受信装置制御部３６に通知する。

【００５９】

受信装置ＩＤ認証部３２は、コンテンツデータ送信装置２０から送信されてきた受信装置ＩＤ情報と受信ＩＤ記憶部３２ａに記憶されている受信装置ＩＤ情報とが一致している場合、受信装置制御部３６の制御により、当該受信装置ＩＤ情報を暗号化して受信装置送受信部３１に出力する。コンテンツデータ送信装置２０から送信されてきた受信装置ＩＤ情報と受信ＩＤ記憶部３２ａに記憶されている受信装置ＩＤ情報とが一致していない場合、受信装置ＩＤ認証部３２は、受信装置ＩＤ情報が一致していない旨の情報（例えば、「０」のデータ）を暗号化して受信装置送受信部３１に出力する。

【００６０】

キー情報抽出部３３は、受信装置送受信部３１が受信したキー情報送信データに格納された情報から暗号化されたキー情報を抽出し、暗号化されたキー情報を復号してキー情報を取得する。キー情報抽出部３３は、キー情報を取得できたか否かを受信装置制御部３６に通知する。キー情報抽出部３３は、受信装置制御部３６の制御により、キー情報を取得できた場合、キー情報を抽出できた旨の情報として、例えば、「１」のデータを暗号化して受信装置送受信部３１に出力し、キー情報を取得できなかった場合、キー情報を抽出できない旨の情報として、例えば、「０」のデータを暗号化して受信装置送受信部３１に出力する。

【００６１】

コンテンツ復号化部３４は、受信装置送受信部３１が受信したコンテンツ送信データから暗号化コンテンツデータを抽出し、キー情報抽出部３３が抽出したキー情報を用いて暗号化コンテンツデータを復号（暗号を解除）する。

【００６２】

出力部３５は、コンテンツ復号化部３４が復号したコンテンツデータをデジタルアナログ変換し、増幅してスピーカに出力する。

【００６３】

受信装置制御部３６は、コンテンツデータ受信装置３０を総合的に制御する。受信装置制御部３６は、受信装置送受信部３１における接続確認データ及び接続確認応答データの送受信、機器認証データ及び機器認証応答データの送受信、キー情報送信データ及びキー情報受信データの送受信、コンテンツ送信データ及びコンテンツ受信データの送受信の制御を行う。

【００６４】

受信装置制御部３６は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信された接続確認データを受信すると、接続確認応答データを受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する制御を行う。

【００６５】

受信装置制御部３６は、受信装置ＩＤ認証部３２がコンテンツデータ送信装置２０から送信されてきた機器認証データの受信装置ＩＤ情報と受信ＩＤ記憶部３２ａに記憶されている受信装置ＩＤ情報とを照合した結果、両方の受信装置ＩＤ情報が一致している旨又は両方の受信装置ＩＤ情報が一致していない旨の情報をコンテンツデータ送信装置２０に送信する制御を行う。

【００６６】

両方の受信装置ＩＤ情報が一致している場合、受信装置制御部３６は、受信装置ＩＤ認証部３２に、受信装置ＩＤ情報を暗号化し、暗号化した受信装置ＩＤ情報を分割し、分割したデータを複数のデータ列からなる機器認証応答データにそれぞれ格納し、機器認証応答データを受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する制御を行う。

【００６７】

両方の受信装置ＩＤ情報が一致しない場合、受信装置制御部３６は、受信装置ＩＤ情報が一致しない旨の情報（例えば、「０」のデータ）を暗号化し、暗号化したデータを複数のデータ列からなる機器認証応答データにそれぞれ格納し、機器認証応答データを受信装置送受信部２５から応答線を介してコンテンツデータ送信装置２０に送信する制御を行う。

【００６８】

受信装置制御部３６は、キー情報抽出部３３がコンテンツデータ送信装置２０から送信されてきたキー情報送信データからキー情報を取得できたか否かを確認し、キー情報抽出部３３がキー情報を取得できた旨又はキー情報抽出部３３がキー情報を取得できなかった旨の情報をコンテンツデータ送信装置２０に送信する制御を行う。

【００６９】

キー情報抽出部３３がキー情報を取得できた場合、受信装置制御部３６は、キー情報を取得できた旨の情報（例えば、「１」のデータ）を暗号化し、暗号化したデータを分割し、分割したデータを複数のデータ列からなるキー情報受信データに格納し、キー情報受信データを受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する制御を行う。

【００７０】

キー情報抽出部３３がキー情報を取得できなかった場合、受信装置制御部３６は、キー情報を取得できなかった旨の情報（例えば、「０」のデータ）を暗号化し、暗号化したデータを分割し、分割したデータを複数のデータ列からなるキー情報受信データに格納し、キー情報受信データを受信装置送受信部３１から応答線を介してコンテンツデータ送信装

置２０に送信する制御を行う。

【００７１】

受信装置制御部３６は、キー情報抽出部３３がキー情報を取得でき、コンテンツデータ送信装置２０からコンテンツ送信データが送信されてくると、コンテンツ送信データに格納されている暗号化コンテンツデータを抽出し、コンテンツ復号化部３４においてキー情報を用いて暗号化コンテンツデータを復号する制御を行う。

【００７２】

受信装置制御部３６は、コンテンツ復号化部３４がコンテンツデータ送信装置２０から送信されてきたコンテンツ送信データから暗号化コンテンツデータを取得して復号できたか否かを確認し、コンテンツ復号化部３４が暗号化コンテンツデータを受信し復号できた旨又はコンテンツ復号化部３４が暗号化コンテンツデータを受信できなかった或いは復号できなかった旨の情報をコンテンツデータ送信装置２０に送信する制御を行う。

【００７３】

コンテンツ復号化部３４が暗号化コンテンツデータを受信し復号できた場合、受信装置制御部３６は、暗号化コンテンツデータを受信し復号できた旨の情報（例えば、「１」のデータ）を暗号化し、暗号化したデータを分割し、分割したデータを複数のデータ列からなるコンテンツ受信データに格納し、コンテンツ受信データを受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する制御を行う。

【００７４】

コンテンツ復号化部３４が暗号化コンテンツデータを受信できなかった或いは復号できなかった場合、受信装置制御部３６は、暗号化コンテンツデータを受信できなかった或いは復号できなかった旨の情報（例えば、「０」のデータ）を暗号化し、暗号化したデータを分割し、分割したデータを複数のデータ列からなるコンテンツ受信データに格納し、コンテンツ受信データを受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する制御を行う。

【００７５】

受信装置制御部３６は、コンテンツ復号化部３４において復号されたコンテンツデータをデジタルアナログ変換し、増幅して出力するよう出力部３５を制御する。

【００７６】

次に、コンテンツデータ送信装置２０とコンテンツデータ受信装置３０との間で伝送されるデータについて説明する。

図２は、本実施例のコンテンツデータ送受信システムにおける接続確認データ及び接続確認応答データのフォーマットを示す図である。図２（ａ）は、コンテンツデータ送信装置からコンテンツデータ受信装置に送信する接続確認データを示し、図２（ｂ）は、コンテンツデータ受信装置からコンテンツデータ送信装置に送信する接続確認応答データを示す。

【００７７】

接続確認データは、図２（ａ）に示すように、送信データ情報領域を備える。送信データ情報領域には、当該データが接続確認のためのデータ（接続確認データ）であることを示す情報が格納される。コンテンツデータ送信装置２０は、図２（ａ）に示す接続確認データを複数のデータ線のうちの１線（本実施例では、第１データ線）を介してコンテンツデータ受信装置３０に送信する。

【００７８】

接続確認応答データは、図２（ｂ）に示すように、送信データ情報領域を備える。送信データ情報領域には、当該データが接続確認データに対する応答データ（接続確認応答データ）であることを示す情報が格納される。コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０からデータ線を介して図２（ａ）に示す接続確認データが送信されてくると、図２（ｂ）に示す接続確認応答データを応答線を介してコンテンツデータ送信装置２０に送信する。

【００７９】

コンテンツデータ送信装置２０は、接続確認データをコンテンツデータ受信装置３０に送信した後、コンテンツデータ受信装置３０から接続確認応答データが送信されてこない場合、コンテンツデータ受信装置３０と接続されていないと判断し、一定時間後に再度送信を行う。

【００８０】

図３は、本実施例のコンテンツデータ送受信システムにおける機器認証データ及び機器認証応答データのフォーマットを示す図である。図３（ａ）は、コンテンツデータ送信装置からコンテンツデータ受信装置に送信する機器認証データを示し、図３（ｂ）は、コンテンツデータ受信装置からコンテンツデータ送信装置に送信する機器認証応答データを示す。

【００８１】

機器認証データは、図３（ａ）に示すように、第１データ列、第２データ列、・・・、第６データ列からなる。各データ列は、暗号化された受信装置ＩＤ情報を分割した情報をそれぞれ格納するデータ領域と、機器認証データに関する情報を格納する送信データ情報領域とを備える。

【００８２】

具体的には、第１データ列において、第１データ領域は、暗号化された受信装置ＩＤ情報を６分割した情報のうちのいずれか１つの情報（第１ＩＤ情報）を格納し、第１送信データ情報領域は、第１データ列～第６データ列のデータ列が機器認証データであることを示す情報を格納する。

【００８３】

第２データ列～第６データ列において、第２データ領域～第６データ領域は、暗号化された受信装置ＩＤ情報を６分割した情報のうちのいずれかの情報（第２ＩＤ情報～第６ＩＤ情報）をそれぞれ格納し、第２送信データ情報領域～第６送信データ情報領域は、機器認証データが第１データ列～第６データ列からなることを示す送信データ確認情報を格納する。

【００８４】

送信データ確認情報は、例えば、チェックサム値である。チェックサム値は、データを１バイト（８ビット）毎に分け、各バイト単位で各ビット数を加算した結果を示す値である。本実施例では、第２データ列は、第１データ列と第２データ列のデータ領域に格納されているデータのチェックサム値と、第１データ列～第６データ列のデータ領域に格納されているデータのチェックサム値とを格納し、第３データ列～第６データ列は、それぞれのデータ列におけるデータ領域に格納されているデータのチェックサム値と、第１データ列～第６データ列のデータ領域に格納されているデータのチェックサム値とを格納するものとする。コンテンツデータ受信装置３０は、送信データ確認情報のチェックサム値を確認することにより複数のデータ列からなる機器認証データを全て受信できたか否かを確認する。

【００８５】

なお、本実施例では、第１データ列の第１送信データ情報領域は、第１データ列～第６データ列のデータ列が機器認証データであることを示す情報を格納し、第２データ列の第２送信データ情報領域～第６データ列の第６送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第１データ列の第１送信データ情報領域～第５データ列の第５送信データ情報領域に第１データ列～第６データ列のデータ列が機器認証データであることを示す情報を格納し、第６データ列の第６送信データ情報領域に第１データ列～第６データ列の送信データ確認情報（第１データ列～第６データ列のチェックサム値）を格納してもよい。

【００８６】

コンテンツデータ送信装置２０は、送信ＩＤ記憶部２４ａが記憶している受信装置ＩＤ情報を暗号化し、暗号化した受信装置ＩＤ情報を分割し、図３（ａ）に示す第１データ列の第１データ領域～第６データ列の第６データ領域にそれぞれ第１ＩＤ情報～第６ＩＤ情

報を格納し、第１データ列～第６データ列をそれぞれ第１データ線～第６データ線を介して同時にコンテンツデータ受信装置３０に送信する。

【００８７】

機器認証応答データは、図３（ｂ）に示すように、第１データ列、第２データ列、・・・、第６データ列からなる。各データ列は、コンテンツデータ受信装置３０において受信装置ＩＤ情報が一致したか否かに関する情報を分割した情報のいずれかの情報を格納するデータ領域と、機器認証応答データに関する情報を格納する送信データ情報領域とを備える。

【００８８】

具体的には、第１データ列の第１データ領域は、暗号化された受信装置ＩＤ情報を６分割した情報のうちのいずれか１つの情報（第１ＩＤ情報）を格納し、第１送信データ情報領域は、第１データ列～第６データ列のデータ列が機器認証応答データであることを示す情報を格納する。

【００８９】

第２データ列の第２データ領域～第６データ列の第６データ領域は、暗号化された受信装置ＩＤ情報を６分割した情報のうちのいずれかの情報（第２ＩＤ情報～第６ＩＤ情報）をそれぞれ格納し、第２送信データ情報領域～第６送信データ情報領域は、機器認証データが第１データ列～第６データ列からなることを示す送信データ確認情報を格納する。送信データ確認情報は、機器確認データの第２データ列～第６データ列と同様に、例えば、チェックサム値である。

【００９０】

なお、本実施例では、第１データ列の第１送信データ情報領域は、第１データ列～第６データ列のデータ列が機器認証応答データであることを示す情報を格納し、第２データ列の第２送信データ情報領域～第６データ列の第６送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第１データ列の第１送信データ情報領域～第５データ列の第５送信データ情報領域に第１データ列～第６データ列のデータ列が機器認証応答データであることを示す情報を格納し、第６データ列の第６送信データ情報領域に第１データ列～第６データ列の送信データ確認情報（第１データ列～第６データ列のチェックサム値）を格納してもよい。

【００９１】

コンテンツデータ受信装置３０において受信装置ＩＤ情報が一致したか否かを示す情報は、コンテンツデータ送信装置２０が送信した受信装置ＩＤ情報とコンテンツデータ受信装置３０に割り当てられている受信装置ＩＤ情報とが一致している場合は、コンテンツデータ受信装置３０の受信ＩＤ記憶部３２ａに記憶されている受信装置ＩＤ情報を暗号化した情報である。当該情報は、分割され、分割された第１ＩＤ情報～第６ＩＤ情報は、第１データ列の第１データ領域～第６データ列の第６データ領域にそれぞれ格納される。

【００９２】

また、コンテンツデータ送信装置２０が送信した受信装置ＩＤ情報とコンテンツデータ受信装置３０に割り当てられている受信装置ＩＤ情報とが一致していない場合は、コンテンツテデータ受信装置３０において受信装置ＩＤ情報が一致したか否かに関する情報は、全て「０」のデータであり、第１データ列の第１データ領域～第６データ列の第６データ領域に「０」のデータが格納される。

【００９３】

本実施例では、コンテンツデータ送信装置２０が送信した受信装置ＩＤ情報とコンテンツデータ受信装置３０に割り当てられている受信装置ＩＤ情報とが一致している場合に、コンテンツテデータ受信装置３０において受信装置ＩＤ情報が一致したか否かに関する情報を、受信装置ＩＤ情報を暗号化した情報としたが、それ以外の情報（例えば、全て「１」のデータ）でもよい。また、本実施例では、コンテンツデータ送信装置２０が送信した受信装置ＩＤ情報とコンテンツデータ受信装置３０に割り当てられている受信装置ＩＤ情報とが一致していない場合に、コンテンツデータ受信装置３０において受信装置ＩＤ情報

が一致したか否かに関する情報を全て「０」のデータとしたが、それ以外の情報（例えば、「１０１０１０・・・」のデータ）でもよい。

【００９４】

コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０から送信された機器認証データを受信すると、第１データ列～第６データ列に格納されている第１ＩＤ情報～第６ＩＤ情報を抽出し、これらの情報を復号し受信装置ＩＤ情報を取得し、受信装置ＩＤ認証部３２の受信ＩＤ記憶部３２ａに記憶している受信装置ＩＤ情報と照合する。コンテンツデータ送信装置２０から送信された受信装置ＩＤ情報と受信ＩＤ記憶部３２ａに記憶された受信装置ＩＤ情報が一致している場合、受信ＩＤ記憶部３２ａに記憶された受信装置ＩＤ情報を暗号化して分割し、図３（ｂ）に示す第１データ列の第１データ領域～第６データ列の第６データ領域に格納し、応答線により、第１データ列～第６データ列を順次コンテンツデータ送信装置２０に送信する。

【００９５】

コンテンツデータ受信装置３０からコンテンツデータ送信装置２０への機器認証データの送信は、第１データ列を送信した後、予め定めた時間経過した後に第２データ列を送信するように、予め定めた時間毎に順次送信してもよい。

【００９６】

機器認証データを応答線で第１データ列～第６データ列を連続して送信した場合、応答線から１つのデータ列として第１データ列～第６データ列とを抽出しやすくなり、抽出したデータから機器の受信装置ＩＤ情報を得ることができやすくなる。そうすると、受信装置ＩＤ情報により設定されている機器以外の機器（例えば、パーソナルコンピュータ）をＤＶＤプレーヤに接続し、抽出した受信装置ＩＤ情報を用いて、パーソナルコンピュータをＤＶＤプレーヤと認識させてキー情報や暗号化コンテンツデータを得て、暗号化コンテンツデータをキー情報により解読し、解読したコンテンツデータを違法に複製記録することができてしまう。

【００９７】

このため、機器認証データの第１データ列を送信した後、予め定めた時間経過後に第２データ列を送信するように、第１データ列～第６データ列をそれぞれ予め定めた間隔毎に送信することにより、応答線から１つのデータ列としてＩＤ情報を抽出しにくくすることができる。

【００９８】

図４は、本実施例のコンテンツデータ送受信システムにおけるキー情報送信データ及びキー情報受信データのフォーマットを示す図である。図４（ａ）は、コンテンツデータ送信装置からコンテンツデータ受信装置に送信するキー情報送信データを示し、図４（ｂ）は、コンテンツデータ受信装置からコンテンツデータ送信装置に送信するキー情報受信データを示す。

【００９９】

キー情報送信データは、図４（ａ）に示すように、第１データ列、第２データ列、・・・、第６データ列からなる。各データ列は、暗号化されたキー情報を分割した情報のいずれかの情報を格納するデータ領域と、キー情報送信データに関する情報を格納する送信データ情報領域とを備える。

【０１００】

具体的には、第１データ列の第１データ領域は、暗号化されたキー情報を６分割した情報のうちのいずれかの１つの情報（第１キー情報）を格納し、第１送信データ情報領域は、第１データ列～第６データ列のデータ列がキー情報送信データであることを示す情報を格納する。

【０１０１】

第２データ列の第２データ領域～第６データ列の第６データ領域は、暗号化されたキー情報情報を６分割した情報のうちのいずれかの情報（第２キー情報～第６キー情報）をそれぞれ格納し、第２送信データ情報領域～第６送信データ情報領域は、キー情報送信デー

タが第１データ列～第６データ列からなることを示す送信データ確認情報を格納する。

【０１０２】

送信データ確認情報は、機器確認データの第２データ列～第６データ列と同様に、例えば、チェックサム値である。コンテンツデータ受信装置３０は、送信データ確認情報のチェックサム値を確認することにより複数のデータ列からなるキー情報送信データを全て受信できたか否かを確認する。

【０１０３】

なお、本実施例では、第１データ列の第１送信データ情報領域は、第１データ列～第６データ列のデータ列がキー情報送信データであることを示す情報を格納し、第２データ列の第２送信データ情報領域～第６データ列の第６送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第１データ列の第１送信データ情報領域～第５データ列の第５送信データ情報領域に第１データ列～第６データ列のデータ列がキー情報送信データであることを示す情報を格納し、第６データ列の第６送信データ情報領域は、第１データ列～第６データ列の送信データ確認情報（第１データ列～第６データ列のチェックサム値）を格納してもよい。

【０１０４】

コンテンツデータ送信装置２０は、図４（ａ）に示すように、暗号化したキー情報を６分割した情報をそれぞれ第１データ列の第１データ領域～第６データ列の第６データ領域に格納し、第１データ列～第６データ列をそれぞれ第１データ線～第６データ線で同時にコンテンツデータ受信装置１０３に送信する。

【０１０５】

キー情報受信データは、図４（ｂ）に示すように、第１データ列、第２データ列、・・・、第６データ列からなる。各データ列は、キー情報を取得したか否かを示す情報を暗号化し、暗号化した情報を分割したいずれかの情報をそれぞれ格納するデータ領域と、キー情報受信データに関する情報を格納する送信データ情報領域とを備える。

【０１０６】

具体的には、第１データ列の第１データ領域は、キー情報を取得したか否かを示す情報を６分割した情報のうちのいずれか１つの情報（第１キー情報）を格納し、第１送信データ情報領域は、第１データ列～第６データ列のデータ列がキー情報受信データであることを示す情報を格納する。

【０１０７】

第２データ列の第２データ領域～第６データ列の第６データ領域は、キー情報を取得したか否かを示す情報を６分割した情報のうちのいずれかの情報（第２キー情報～第６キー情報）をそれぞれ格納し、第２送信データ情報領域～第６送信データ情報領域は、機器認証データが第１データ列～第６データ列からなることを示す送信データ確認情報を格納する。送信データ確認情報は、機器確認データの第２データ列～第６データ列と同様に、例えば、チェックサム値である。

【０１０８】

キー情報を取得したか否かを示す情報は、例えば、コンテンツデータ受信装置３０がキー情報を取得した場合、全て「１」のデータであり、コンテンツデータ受信装置３０がキー情報を取得できなかった場合、全て「０」のデータである。

【０１０９】

なお、本実施例では、第１データ列の第１送信データ情報領域は、第１データ列～第６データ列のデータ列がキー情報受信データであることを示す情報を格納し、第２データ列の第２送信データ情報領域～第６データ列の第６送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第１データ列の第１送信データ情報領域～第５データ列の第５送信データ情報領域に第１データ列～第６データ列のデータ列がキー情報受信データであることを示す情報を格納し、第６データ列の第６送信データ情報領域は、第１データ列～第６データ列の送信データ確認情報（第１データ列～第６データ列のチェックサム値）を格納してもよい。

【０１１０】
コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０が送信したキー情報を取得できた場合、第１データ列の第１データ領域～第６データ列の第６データ領域の全てのビットに「１」のデータを格納し、コンテンツデータ送信装置２０に応答線を介して、第１データ列～第６データ列を順次送信する。
【０１１１】
コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０が送信したキー情報を取得できなかった場合、コンテンツデータ受信装置３０は、第１データ列の第１データ領域～第６データ列の第６データ領域の全てのビットに「０」のデータを格納し、コンテンツデータ送信装置２０に応答線を介して、第１データ列～第６データ列を順次送信する。
【０１１２】
本実施例では、キー情報の取得に関する情報は、コンテンツデータ受信装置３０がキー情報の取得した場合に全て「１」のデータとし、コンテンツデータ受信装置３０がキー情報の取得できなかった場合に全て「０」のデータとするが、それに限定されない。例えば、コンテンツデータ受信装置３０がキー情報の取得した場合に、第１データ列の第１データ領域～第６データ列の第６データ領域の各データ領域の半分のビットを「１」のデータとし、残りの半分のビットを「０」のデータとするなど、キー情報を取得できた場合とキー情報を取得できなかった場合とが区別できれば、他のパターンのデータであってもよい。
【０１１３】
また、コンテンツデータ受信装置３０がコンテンツデータ送信装置２０に応答線を介してキー情報受信データを送信する際、上述した機器認証応答データの同様に、コンテンツデータ受信装置３０は、第１データ列～第６データ列を、予め定めた時間間隔で順次送信してもよい。
【０１１４】
また、本実施例では、キー情報受信データは、複数のデータ列からなるものとしたが、キー情報を取得したか否かを示す情報を格納するデータ領域と、当該データ列がキー情報受信データであることを示す情報を格納する送信データ情報領域とからなる一つのデータ列であってもよい。
【０１１５】
図５は、本実施例のコンテンツデータ送受信システムにおけるコンテンツ送信データ及びコンテンツ受信データのフォーマットを示す図である。図５（ａ）は、コンテンツデータ送信装置からコンテンツデータ受信装置に送信するコンテンツ送信データを示し、図５（ｂ）は、コンテンツデータ受信装置からコンテンツデータ送信装置に送信するコンテンツ受信データを示す。
【０１１６】
コンテンツ送信データは、図４（ａ）に示すように、第１データ列、第２データ列、・・・、第６データ列からなる。各データ列は、暗号化されたコンテンツデータを分割し、分割した情報のいずれかの情報を格納するデータ領域と、コンテンツ送信データに関する情報を格納する送信データ情報領域とを備える。
【０１１７】
具体的には、第１データ列の第１データ領域は、暗号化コンテンツデータを６分割した情報のうちのいずれかの１つの情報（第１コンテンツ情報）を格納し、第１送信データ情報領域は、第１データ列～第６データ列のデータ列がコンテンツ送信データであることを示す情報を格納する。
【０１１８】
第２データ列の第２データ領域～第６データ列の第６データ領域は、暗号化コンテンツデータを６分割した情報のうちのいずれかの情報（第２コンテンツ情報～第６コンテンツ情報）をそれぞれ格納し、第２送信データ情報領域～第６送信データ情報領域は、コンテ

ンツ送信データが第１データ列～第６データ列からなることを示す送信データ確認情報を格納する。

【０１１９】

送信データ確認情報は、キー情報送信データの第２データ列～第６データ列と同様に、例えば、チェックサム値である。コンテンツデータ受信装置３０は、送信データ確認情報のチェックサム値を確認することにより複数のデータ列からなるコンテンツ送信データを全て受信できたか否かを確認する。

【０１２０】

なお、本実施例では、第１データ列の第１送信データ情報領域は、第１データ列～第６データ列のデータ列がコンテンツ送信データであることを示す情報を格納し、第２データ列の第２送信データ情報領域～第６データ列の第６送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第１データ列の第１送信データ情報領域～第５データ列の第５送信データ情報領域に第１データ列～第６データ列のデータ列がコンテンツ送信データであることを示す情報を格納し、第６データ列の第６送信データ情報領域は、第１データ列～第６データ列の送信データ確認情報（第１データ列～第６データ列のチェックサム値）を格納してもよい。

【０１２１】

本実施例では、暗号化されたコンテンツデータを分割し、分割したそれぞれの情報を各データ列の各データ領域に格納するとしたが、それに限定されない。例えば、コンテンツデータがマルチチャンネルのオーディオデータの場合、レフト、ライト、サラウンドレフト、サラウンドライト、センター、サブウーハーのオーディオデータは、それぞれチャンネル毎に暗号化され、暗号化レフト、暗号化ライト、暗号化サラウンドレフト、暗号化サラウンドライト、暗号化センター、暗号化サブウーハーのデータとなり、これらの暗号化コンテンツデータをそれぞれ第１データ列の第１データ領域～第６データ列の第６データ領域にそれぞれ格納するようにしてもよい。

【０１２２】

コンテンツデータ送信装置２０は、図５（ａ）に示すように、第１データ列の第１データ領域～第６データ列の第６データ領域に、暗号化コンテンツデータをそれぞれ格納し、第１データ列～第６データ列をそれぞれ第１データ線～第６データ線を介して同時にコンテンツデータ受信装置３０に送信する。

【０１２３】

本実施例においては、コンテンツデータ送信装置２０からコンテンツデータ受信装置３０への暗号化コンテンツデータの送信は、上述したように、暗号化コンテンツデータをデータ領域と送信データ情報領域とからなるデータ列に格納し、第１データ列～第６データ列を１回の送信として行うが、１回目に送信データ情報領域のみからなるデータ列をヘッダとして送信し、そのデータ列に連続してデータ領域のみからなるデータ列を送信する方法であってもよい。

【０１２４】

この場合、２回目以降のコンテンツ送信データの送信において、１回の送信により送信できる暗号化コンテンツテータのデータ量が、上述した図５（ａ）のフォーマットで送信する暗号化コンテンツデータのデータ量より多いため、コンテンツデータ送信装置２０からコンテンツデータ受信装置３０に、より短時間ので多くの暗号化コンテンツデータを送信することができる。

【０１２５】

コンテンツ受信データは、図５（ｂ）に示すように、第１データ列、第２データ列、・・・、第６データ列からなる。各データ列は、暗号化コンテンツデータを受信できた否かを示す情報を暗号化し、暗号化した情報を分割したいずれかの情報をそれぞれ格納するデータ領域と、コンテンツ受信データに関する情報を格納する送信データ情報領域とを備える。

【０１２６】

具体的には、第１データ列の第１データ領域は、暗号化コンテンツデータを受信できたか否かを示す情報を６分割した情報のうちのいずれか１つの情報（第１コンテンツ情報）を格納し、第１送信データ情報領域は、第１データ列～第６データ列のデータ列がコンテンツ受信データであることを示す情報を格納する。

【０１２７】

第２データ列の第２データ領域～第６データ列の第６データ領域は、暗号化コンテンツデータを受信できたか否かを示す情報を６分割した情報のうちのいずれかの情報（第２コンテンツ情報～第６コンテンツ情報）をそれぞれ格納し、第２送信データ情報領域～第６送信データ情報領域は、コンテンツ受信データが第１データ列～第６データ列からなることを示す送信データ確認情報を格納する。送信データ確認情報は、キー情報受信データの第２データ列～第６データ列と同様に、例えば、チェックサム値である。

【０１２８】

なお、本実施例では、第１データ列の第１送信データ情報領域は、第１データ列～第６データ列のデータ列がコンテンツ受信データであることを示す情報を格納し、第２データ列の第２送信データ情報領域～第６データ列の第６送信データ情報領域は、送信データ確認情報を格納するとしたが、それに限定されない。例えば、第１データ列の第１送信データ情報領域～第５データ列の第５送信データ情報領域に第１データ列～第６データ列のデータ列がコンテンツ受信データであることを示す情報を格納し、第６データ列の第６送信データ情報領域は、第１データ列～第６データ列の送信データ確認情報（第１データ列～第６データ列のチェックサム値）を格納してもよい。

【０１２９】

暗号化コンテンツデータを受信できたか否かを示す情報は、例えば、コンテンツデータ受信装置３０が暗号化コンテンツデータを受信した場合、全て「１」のデータであり、コンテンツデータ受信装置３０が暗号化コンテンツデータを受信できなかった場合、全て「０」のデータである。

【０１３０】

コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０が送信した暗号化コンテンツデータを受信できた場合、第１データ列の第１データ領域～第６データ列の第６データ領域の全てのビットに「１」のデータを格納し、コンテンツデータ送信装置２０に応答線を介して、第１データ列～第６データ列を順次送信する。

【０１３１】

コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０が送信した暗号化コンテンツデータを受信できなかった場合、コンテンツデータ受信装置３０は、第１データ列の第１データ領域～第６データ列の第６データ領域の全てのビットに「０」のデータを格納し、コンテンツデータ送信装置２０に応答線を介して第１データ列～第６データ列を順次送信する。

【０１３２】

本実施例では、キー情報の取得に関する情報は、コンテンツデータ受信装置３０が暗号化コンテンツデータを受信した場合に全て「１」のデータとし、コンテンツデータ受信装置２０が暗号化コンテンツデータを受信できなかった場合に全て「０」のデータとするが、それに限定されない。例えば、コンテンツデータ受信装置２０が暗号化コンテンツデータを受信した場合に、第１データ列の第１データ領域～第６データ列の第６データ領域の各データ領域の半分のビットを「１」のデータとし、残りの半分のビットを「０」のデータとするなど、暗号化コンテンツデータを受信できた場合と暗号化コンテンツデータを受信できなかった場合とが区別できれば、他のパターンのデータであってもよい。

【０１３３】

また、コンテンツデータ受信装置３０がコンテンツデータ送信装置２０に応答線を介してコンテンツ受信データを送信する際、上述した機器認証応答データの同様に、コンテンツデータ受信装置３０は、第１データ列～第６データ列を、予め定めた時間間隔で順次送信してもよい。

【０１３４】
また、本実施例では、コンテンツ受信データは、複数のデータ列からなるものとしたが、暗号化コンテンツデータを受信したか否かを示す情報を格納するデータ領域と、当該データ列がコンテンツ受信データであることを示す情報を格納する送信データ情報領とからなる一つのデータ列であってもよい。
【０１３５】
また、本実施例では、コンテンツ受信データは、コンテンツデータ受信装置３０がコンテンツ送信データを受信する毎にコンテンツデータ送信装置２０に送信するとしたが、それに限定されない。コンテンツデータ送信装置２０がコンテンツ送信データの送信を開始した後、コンテンツデータ受信装置３０は、予め定めた時間毎にコンテンツデータ送信装置２０にコンテンツ受信データを送信するようにしてもよい。または、コンテンツデータ送信装置２０がコンテンツ送信データの送信を開始した後、コンテンツデータ受信装置３０は、コンテンツ送信データを受信する間隔が予め定めた時間以上経過した場合にコンテンツデータ送信装置２０にコンテンツ受信データを送信するようにしてもよい。
【０１３６】
次に、本実施例のコンテンツデータ送受信システムにおけるデータの送受信の流れについて説明する。
図６は、本発明のコンテンツデータ送受信方法の一実施例を説明するための図である。図６において、図の縦軸は、時間の流れを示す。
【０１３７】
コンテンツデータ送信装置２０は、コンテンツデータ送信装置２０とコンテンツデータ受信装置３０とが信号線により接続されているか否かを確認するため、図２（ａ）に示す接続確認データを、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。
【０１３８】
コンテンツデータ受信装置３０は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信された接続確認データを受信すると、図２（ｂ）に示す接続確認応答データを受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。
【０１３９】
コンテンツデータ送信装置２０は、送信装置送受信部２５がコンテンツデータ受信装置３０から送信された接続確認応答データを受信すると、送信装置ＩＤ認証部２４の送信ＩＤ記憶部２４ａに記憶しているコンテンツデータ受信装置毎に固有に割り当てられている複数の受信装置ＩＤ情報から１つの受信装置ＩＤ情報を抽出し、抽出した受信装置ＩＤ情報を暗号化し、暗号化した受信装置ＩＤ情報を分割して図３（ａ）に示す機器認証データに格納し、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。
【０１４０】
コンテンツデータ受信装置３０は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信された機器認証データを受信すると、機器認証データの中からＩＤ情報領域に格納されている受信装置ＩＤ情報を抽出し、抽出した受信装置ＩＤ情報を復号し、復号した受信装置ＩＤ情報と受信装置ＩＤ認証部３２の受信ＩＤ記憶部３２ａに記憶されている受信装置ＩＤ情報とを照合する。
【０１４１】
機器認証データから抽出した受信装置ＩＤ情報と受信ＩＤ記憶部３２ａに記憶している受信装置ＩＤ情報とが一致した場合、コンテンツデータ受信装置３０は、当該受信装置ＩＤ情報を暗号化し、暗号化したデータを分割し、図３（ｂ）に示す機器認証応答データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。
【０１４２】
機器認証データから抽出した受信装置ＩＤ情報と受信ＩＤ記憶部３２ａに記憶している

受信装置ＩＤ情報とが一致しない場合、コンテンツデータ受信装置３０は、受信ＩＤ情報が一致しない旨の情報（例えば、全て「０」のデータ）を暗号化し、暗号化したデータを分割して図３（ｂ）に示す機器認証応答データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１４３】

コンテンツデータ送信装置２０は、送信装置送受信部２５がコンテンツデータ受信装置３０から送信された機器認証応答データを受信すると、機器認証応答データに格納されているデータを抽出し、そのデータからコンテンツデータ受信装置３０において受信情報ＩＤ情報が一致したか否か確認する。

【０１４４】

機器認証データから得たデータがコンテンツデータ受信装置３０において受信装置ＩＤ情報が一致した旨の情報の場合、コンテンツデータ送信装置２０は、コンテンツ再生部２１においてコンテンツデータの再生を開始し、コンテンツ暗号化部２２においてキー情報生成部２３がキー情報を用いてコンテンツデータを暗号化する処理を開始する。

【０１４５】

コンテンツデータ送信装置２０は、コンテンツデータの暗号化を開始すると共に、キー情報生成部２３により生成されたキー情報を暗号化し、暗号化したデータを分割して図４（ａ）に示すキー情報送信データに格納し、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０１４６】

機器認証データから得たデータがコンテンツデータ受信装置３０において受信装置ＩＤ情報が一致しない旨の情報の場合、コンテンツデータ送信装置２０は、送信装置ＩＤ認証部２４の送信ＩＤ記憶部２４ａに記憶している複数の受信装置ＩＤ情報の中から、既にコンテンツデータ受信装置３０に送信した受信装置ＩＤ情報を除く受信装置ＩＤ情報の中から１つの受信装置ＩＤ情報を抽出し、その受信装置ＩＤ情報を暗号化し、暗号化したデータを分割して図３（ａ）に示す機器認証データに格納し、再度、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。コンテンツデータ送信装置２０は、コンテンツデータ受信装置３０に割り当てられた受信装置ＩＤ情報と一致するまでこの処理を繰り返し行う。

【０１４７】

コンテンツデータ受信装置３０は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信されたキー情報送信データを受信すると、キー情報送信データの中からキー情報領域に格納されているデータを抽出し、抽出したデータを復号化しキー情報を取得する。このキー情報が暗号化コンテツデータの暗号を解除する暗号解除情報となる。

【０１４８】

キー情報送信データからキー情報を取得することができた場合、コンテンツデータ受信装置３０は、キー情報を取得した旨の情報（例えば、全て「１」のデータ）を暗号化し、暗号化したデータを分割して図４（ｂ）に示すキー情報受信データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１４９】

キー情報送信データからキー情報を取得できなかった場合、コンテンツデータ受信装置３０は、キー情報を取得できなかった旨の情報（例えば、全て「０」のデータ）を暗号化し、暗号化したデータを分割して図４（ｂ）に示すキー情報受信データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１５０】

コンテンツデータ送信装置２０は、送信装置送受信部２５がコンテンツデータ受信装置３０から送信されたキー情報受信データを受信すると、キー情報受信データの受信データ領域に格納されているデータを抽出し、コンテンツデータ受信装置３０がキー情報を取得したか否かを確認する。

【０１５１】

コンテンツデータ受信装置３０においてキー情報を取得できなかった場合、コンテンツデータ送信装置２０は、再度、キー情報送信データを送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０１５２】

コンテンツデータ受信装置３０においてキー情報を取得できた場合、コンテンツデータ送信装置２０は、コンテンツ暗号化部２２により暗号化した暗号化コンテンツデータを分割し、分割したデータを図５（ａ）に示すコンテンツ送信データに格納し、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０１５３】

コンテンツデータ受信装置３０においてキー情報を取得できなかった場合、コンテンツデータ受信装置３０は、コンテンツデータを取得できなかった旨の情報（例えば、全て「０」のデータ）を暗号化し、暗号化したデータを分割して図５（ｂ）に示すコンテンツ受信データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１５４】

コンテンツデータ受信装置３０は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信されたコンテンツ送信データを受信すると、コンテンツ送信データに格納されている暗号化コンテンツデータを抽出し、コンテンツ復号化部３４においてキー情報抽出部３３が抽出したキー情報を用いて暗号化コンテンツデータを復号化し、出力部３５に出力する。

【０１５５】

出力部３５は、コンテンツ復号化部３４から出力されたコンテンツデータに対して、デジタルアナログ変換や増幅等を行い出力する。

【０１５６】

コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０が送信したコンテンツ送信データを受信し暗号化コンテンツデータを復号すると、暗号コンテンツデータを取得した旨の情報を暗号化し、暗号化したデータを分割して図５（ｂ）に示すコンテンツ受信データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１５７】

コンテンツデータ送信装置２０は、コンテンツデータ受信装置３０から送信されたコンテンツ受信データを受信すると、コンテンツ受信データに格納されているコンテンツデータを取得した旨の情報からコンテンツデータ受信装置３０がコンテンツデータを取得できたか否かを確認する。

【０１５８】

コンテンツデータ送信装置２０は、コンテンツデータ受信装置３０がコンテンツデータを取得できた場合、次の暗号化コンテンツデータを図５（ａ）に示すコンテンツ送信データに格納し、コンテンツ送信データを送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０１５９】

コンテンツデータ送信装置２０は、コンテンツデータ受信装置３０がコンテンツデータを取得できなかった場合、送信したコンテンツ送信データを、再度、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０１６０】

このようにして、コンテンツデータ送信装置２０からコンテンツデータ受信装置３０にコンテンツデータを送信する。

【０１６１】

以上のように、コンテンツデータ送受信システムにおいて、コンテンツデータ送信装置は、機器認証を行うための受信装置ＩＤ情報、コンテンツデータを復号するためのキー情

報、コンテンツデータを暗号化し、暗号化したデータを複数のデータ列からなるそれぞれのデータに格納し、そのデータを複数の信号線を用いてコンテンツデータ受信装置に送信する。

【０１６２】

このことにより、コンテンツデータ送信装置が出力する受信装置ＩＤ情報、キー情報、暗号化コンテンツデータを単一の信号線から取得することができないため、不正に受信装置ＩＤ情報、キー情報、暗号化コンテンツデータを得て、暗号化コンテンツデータをキー情報を用いて復号してコンテンツデータの違法複製することを防止することができる。

【０１６３】

前述した実施例では、コンテンツデータ送信装置２０は、コンテンツデータを１つのキー情報を用いて暗号化し、コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０から送信されてきた１つのキー情報を用いて暗号化コンテンツデータを復号化しているが、コンテンツデータの暗号化を複数のキー情報を用いて行うようにしてもよい。

【０１６４】

本発明において、コンテンツデータの暗号化を複数のキー情報を用いて行う場合の実施例について説明する。

図７は、本発明のコンテンツデータ送受信システムの他の実施例を示す概略構成図である。

コンテンツデータ送信装置２０は、コンテンツ再生部２１、コンテンツ暗号化部２２、キー情報生成部２３、送信装置ＩＤ認証部２４、送信装置送受信部２５、送信装置制御部２６を備える。このうち、コンテンツ再生部２１、コンテンツ暗号化部２２、送信装置ＩＤ認証部２４及び送信装置制御部２６は、前述した実施例のコンテンツデータ送信装置２０のコンテンツ再生部２１、コンテンツ暗号化部２２、送信装置ＩＤ認証部２４及び送信装置制御部２６と同様の構成であるため、説明を省略する。

【０１６５】

キー情報生成部２３は、コンテンツデータの暗号化に用いる複数のキー情報を生成する。キー情報は、例えば、複数ビットのデータ列からなる情報であり、キー情報の生成方法は特に限定されずどのような方法でもよい。

【０１６６】

キー情報生成部２３は、キー情報生成制御部２３ａを備える。キー情報生成制御部２３ａは、キー情報生成部２３内部で生成された複数のキー情報を記憶する記憶部（図示せず）と、記憶部に記憶した複数のキー情報から１つのキー情報を選択する間隔の時間を計測するためのタイマを備える。

【０１６７】

キー情報生成制御部２３ａは、キー情報生成部２３内部で生成された複数のキー情報を記憶部に記憶し、キー情報をコンテンツデータ受信装置３０に送信する場合に、生成した複数のキー情報のそれぞれを暗号化し、暗号化した複数のキー情報を全て送信装置送受信部２５に出力する。

【０１６８】

キー情報生成部２３におけるキー情報の暗号化は、予め定められた方法により行われる。後述するコンテンツデータ受信装置３０のキー情報抽出部３３は、キー情報生成部２３により行われたキー情報の暗号化を解除する復号処理機能を備え、キー情報生成部２３が暗号化したキー情報は、後述するキー情報抽出部３３により復号が可能である。本実施例では、キー情報生成部２３がキー情報を暗号化してコンテンツデータ受信装置３０に送信するが、暗号化せずにキー情報をコンテンツデータ受信装置３０に送信するようにしてもよい。

【０１６９】

キー情報生成制御部２３ａは、記憶部に記憶した複数のキー情報のうち、コンテンツデータの暗号化に用いる１つのキー情報を選択し、選択したキー情報をコンテンツ暗号化部

２２に出力すると共に、選択したキー情報に関する選択情報を送信装置送受信部２５に出力する。選択情報は、複数のキー情報のうちのどのキー情報であるかを示す情報であり、例えば、１、２の番号などである。キー情報生成制御部２３ａにおけるキー情報の選択方法は、特に限定されず、複数のキー情報を１番目から順番に選択してもよく、また、ランダムに選択してもよい。

【０１７０】

キー情報生成制御部２３ａは、コンテンツ再生部２１においてコンテンツデータの再生が開始した時、記憶部に記憶した複数のキー情報のうちから１つのキー情報を選択し、選択したキー情報をコンテンツ暗号化部２２に出力すると共に、タイマにより時間の計測を開始する。キー情報を選択してから予め定めた時間の経過毎に、新たに、記憶部に記憶した他のキー情報のうちから１つのキー情報を選択し、選択したキー情報をコンテンツ暗号化部２２に出力する。コンテンツ暗号化部２２は、キー情報生成部２３から入力するあたらなキー情報に基づいてコンテンツデータの暗号化を行う。また、キー情報生成部２３は、キー情報を選択する毎に、選択したキー情報に関する選択情報を送信装置送受信部２５に出力する。

【０１７１】

送信装置送受信部２５は、前述した実施例のコンテンツデータ送信装置２０の送信装置送受信部２５の機能を備え、更に、キー情報送信データを送信する際に、キー情報生成部２３から送られてきた複数のキー情報をキー情報送信データに格納してコンテンツデータ受信装置３０に送信する。複数のキー情報をキー情報送信データに格納するとき、複数のキー情報を暗号化して格納してもよく、また、複数のキー情報のそれぞれを分割し、データの順番を入れ替えて複数のデータ列にそれぞれ格納してもよく、また、暗号化せずに格納してもよい。

【０１７２】

また、送信装置送受信部２５は、コンテンツ暗号化部２２から送られてきた暗号化コンテンツデータをコンテンツ送信データに格納して送信する際に、キー情報生成部２３から入力する選択情報もコンテンツ送信データに格納し、コンテンツデータ受信装置３０に送信する。選択情報は、コンテンツ送信データの第１データ列の第１送信データ情報領域～第６データ列の第６送信データ情報領域の全てに格納してもよく、また、いずれかに格納してもよい。

【０１７３】

このように本実施例のコンテンツデータ送信装置２０は、キー情報生成部２３において複数のキー情報を生成し、キー情報をコンテンツデータ受信装置３０に送信する際に、キー情報送信データに複数のキー情報の全てを格納し、コンテンツデータ受信装置３０に送信する。また、キー情報生成部２３では、予め定めた時間毎に複数のキー情報の中から１つのキー情報を選択し、選択したキー情報をコンテンツ暗号化部２２に出力すると共に、選択したキー情報に関する選択情報を送信装置送受信部２５に出力する。

【０１７４】

コンテンツ暗号化部２２は、キー情報生成部２３から予め定めた時間間隔毎に送られてくるキー情報に基づいてコンテンツデータを暗号化し、送信装置送受信部２５に出力する。送信装置送受信部２５は、コンテンツ暗号化部２２から送られてくる暗号化コンテンツデータと、キー情報生成部２３から送られてくるキー情報に関する選択情報とを、コンテンツ送信データに格納し、コンテンツデータ受信装置３０に送信する。

【０１７５】

すなわち、コンテンツデータ送信装置２０は、コンテンツデータを予め定めた時間毎に異なるキー情報で暗号化し、その暗号化コンテンツデータと暗号化に用いたキー情報に関する選択情報とをコンテンツデータ受信装置３０に送信する。

【０１７６】

コンテンツデータ受信装置３０は、受信装置送受信部３１、受信装置ＩＤ認証部３２、キー情報抽出部３３、コンテンツ復号化部３４、出力部３５、受信装置制御部３６を備え

る。このうち、受信装置ＩＤ認証部３２、コンテンツ復号化部３４、出力部３５、受信装置制御部３６は、前述した実施例のコンテンツデータ受信装置３０の受信装置ＩＤ認証部３２、コンテンツ復号化部３４、出力部３５及び受信装置制御部３６と同様であるため、説明を省略する。

【０１７７】

受信装置送受信部３１は、前述した実施例の受信装置送受信部３１の機能を備え、更に、コンテンツ送信データを受信した場合にコンテンツ送信データに含まれる選択情報をキー情報抽出部３３に出力する処理を行う。

【０１７８】

キー情報抽出部３３は、受信装置送受信部３１が受信したキー情報送信データに格納されている複数のキー情報を抽出し、キー情報を取得する。キー情報抽出部３３は、キー情報記憶部３３ａを備え、取得したキー情報をキー情報記憶部３３ａに格納する。

【０１７９】

キー情報抽出部３３は、コンテンツデータ送信装置２０からコンテンツ送信データが送られてきた際に、コンテンツ送信データに含まれる選択情報に基づいて、キー情報記憶部３３ａに記憶している複数のキー情報から１つのキー情報を選択し、選択したキー情報をコンテンツ復号化部３４に出力する。

【０１８０】

このようにコンテンツデータ受信装置３０は、コンテンツデータ送信装置２０から送られてきた複数のキー情報をキー情報記憶部３３ａに記憶し、その後、暗号化コンテンツデータと共に送られてくる選択情報に基づいて、複数のキー情報の中から１つのキー情報を選択し、そのキー情報を用いて暗号化コンテンツデータを復号する。

【０１８１】

次に、本発明の他の本実施例のコンテンツデータ送受信システムにおけるデータの送受信の流れについて説明する。

図６において、コンテンツデータ送信装置２０は、コンテンツデータ送信装置２０とコンテンツデータ受信装置３０とが信号線により接続されているか否かを確認するため、図２（ａ）に示す接続確認データを、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０１８２】

コンテンツデータ受信装置３０は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信された接続確認データを受信すると、図２（ｂ）に示す接続確認応答データを受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１８３】

コンテンツデータ送信装置２０は、送信装置送受信部２５がコンテンツデータ受信装置３０から送信された接続確認応答データを受信すると、送信装置ＩＤ認証部２４の送信ＩＤ記憶部２４ａに記憶しているコンテンツデータ受信装置毎に固有に割り当てられている複数の受信装置ＩＤ情報から１つの受信装置ＩＤ情報を抽出し、抽出した受信装置ＩＤ情報を暗号化し、暗号化した受信装置ＩＤ情報を分割して図３（ａ）に示す機器認証データに格納し、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０１８４】

コンテンツデータ受信装置３０は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信された機器認証データを受信すると、機器認証データの中からＩＤ情報領域に格納されている受信装置ＩＤ情報を抽出し、抽出した受信装置ＩＤ情報を復号し、復号した受信装置ＩＤ情報と受信装置ＩＤ認証部３２の受信ＩＤ記憶部３２ａに記憶されている受信装置ＩＤ情報とを照合する。

【０１８５】

機器認証データから抽出した受信装置ＩＤ情報と受信ＩＤ記憶部３２ａに記憶している受信装置ＩＤ情報とが一致した場合、コンテンツデータ受信装置３０は、当該受信装置Ｉ

Ｄ情報を暗号化し、暗号化したデータを分割し、図３（ｂ）に示す機器認証応答データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１８６】

機器認証データから抽出した受信装置ＩＤ情報と受信ＩＤ記憶部３２ａに記憶している受信装置ＩＤ情報とが一致しない場合、コンテンツデータ受信装置３０は、受信ＩＤ情報が一致しない旨の情報（例えば、全て「０」のデータ）を暗号化し、暗号化したデータを分割して図３（ｂ）に示す機器認証応答データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１８７】

コンテンツデータ送信装置２０は、送信装置送受信部２５がコンテンツデータ受信装置３０から送信された機器認証応答データを受信すると、機器認証応答データに格納されているデータを抽出し、そのデータからコンテンツデータ受信装置３０において受信情報ＩＤ情報が一致したか否か確認する。

【０１８８】

機器認証データから得たデータがコンテンツデータ受信装置３０において受信装置ＩＤ情報が一致した旨の情報の場合、コンテンツデータ送信装置２０は、キー情報生成部２３において複数のキー情報を生成し、生成した複数のキー情報を暗号化し、暗号化したデータを分割して図４（ａ）に示すキー情報送信データに格納し、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０１８９】

機器認証データから得たデータがコンテンツデータ受信装置３０において受信装置ＩＤ情報が一致しない旨の情報の場合、コンテンツデータ送信装置２０は、送信装置ＩＤ認証部２４の送信ＩＤ記憶部２４ａに記憶している複数の受信装置ＩＤ情報の中から、既にコンテンツデータ受信装置３０に送信した受信装置ＩＤ情報を除く受信装置ＩＤ情報の中から１つの受信装置ＩＤ情報を抽出し、その受信装置ＩＤ情報を暗号化し、暗号化したデータを分割して図３（ａ）に示す機器認証データに格納し、再度、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。コンテンツデータ送信装置２０は、コンテンツデータ受信装置３０に割り当てられた受信装置ＩＤ情報と一致するまでこの処理を繰り返し行う。

【０１９０】

コンテンツデータ受信装置３０は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信されたキー情報送信データを受信すると、キー情報送信データの中からキー情報領域に格納されているデータを抽出し、抽出したデータを復号化し、複数のキー情報を取得する。このキー情報を、キー情報記憶部３２ａに記憶する。

【０１９１】

キー情報送信データからキー情報を取得することができた場合、コンテンツデータ受信装置３０は、キー情報を取得した旨の情報（例えば、全て「１」のデータ）を暗号化し、暗号化したデータを分割して図４（ｂ）に示すキー情報受信データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１９２】

キー情報送信データからキー情報を取得できなかった場合、コンテンツデータ受信装置３０は、キー情報を取得できなかった旨の情報（例えば、全て「０」のデータ）を暗号化し、暗号化したデータを分割して図４（ｂ）に示すキー情報受信データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。

【０１９３】

コンテンツデータ送信装置２０は、送信装置送受信部２５がコンテンツデータ受信装置３０から送信されたキー情報受信データを受信すると、キー情報受信データの受信データ領域に格納されているデータを抽出し、コンテンツデータ受信装置３０がキー情報を取得したか否かを確認する。

【０１９４】
コンテンツデータ受信装置３０においてキー情報を取得できなかった場合、コンテンツデータ送信装置２０は、再度、キー情報送信データを送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。
【０１９５】
コンテンツデータ受信装置３０においてキー情報を取得できた場合、コンテンツデータ送信装置２０は、コンテンツ再生部２１においてコンテンツデータの再生を開始すると共に、キー情報生成部２３においてコンテンツデータり暗号化に用いるキー情報の選択を行う。そして、コンテンツ暗号化部２２において選択されたキー情報を用いてコンテンツデータを暗号化する処理を開始する。
【０１９６】
コンテンツデータ送信装置２０は、コンテンツ暗号化部２２により暗号化した暗号化コンテンツデータを分割し、分割したデータを図５（ａ）に示すコンテンツ送信データに格納し、また、キー情報生成部２３から得られる選択情報をコンテツ送信データに格納し、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。
【０１９７】
コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０が送信したコンテンツ送信データを取得できなかった場合、コンテンツデータを取得できなかった旨の情報（例えば、全て「０」のデータ）を暗号化し、暗号化したデータを分割して図５（ｂ）に示すコンテンツ受信データに格納し、受信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。
【０１９８】
コンテンツデータ受信装置３０は、受信装置送受信部３１がコンテンツデータ送信装置２０から送信されたコンテンツ送信データを受信すると、コンテンツ送信データに格納されている選択情報を抽出してキー情報抽出部３３に出力すると共に暗号化コンテンツデータをコンテンツ復号化部３４に出力する。キー情報抽出部３３は、選択情報に基づいてキー情報記憶部３３ａに記憶されている複数のキー情報から１つのキー情報を選択する。そして、コンテンツ復号化部３４は、キー情報抽出部３３が選択したキー情報を用いて暗号化コンテンツデータを復号化し、出力部３５に出力する。
【０１９９】
出力部３５は、コンテンツ復号化部３４から出力されたコンテンツデータに対して、デジタルアナログ変換や増幅等を行い出力する。
【０２００】
コンテンツデータ受信装置３０は、コンテンツデータ送信装置２０が送信したコンテンツ送信データを受信し暗号化コンテンツデータを復号すると、暗号コンテンツデータを取得した旨の情報を暗号化し、暗号化したデータを分割して図５（ｂ）に示すコンテンツ受信データに格納し、送信装置送受信部３１から応答線を介してコンテンツデータ送信装置２０に送信する。
【０２０１】
コンテンツデータ送信装置２０は、コンテンツデータ受信装置３０から送信されたコンテンツ受信データを受信すると、コンテンツ受信データに格納されているコンテンツデータを取得した旨の情報からコンテンツデータ受信装置３０がコンテンツデータを取得できたか否かを確認する。
【０２０２】
コンテンツデータ送信装置２０は、コンテンツデータ受信装置３０がコンテンツデータを取得できた場合、次の暗号化コンテンツデータを図５（ａ）に示すコンテンツ送信データに格納し、コンテンツ送信データを送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。
【０２０３】

コンテンツデータ送信装置２０は、コンテンツデータ受信装置３０がコンテンツデータを取得できなかった場合、送信したコンテンツ送信データを、再度、送信装置送受信部２５から第１データ線～第６データ線を介してコンテンツデータ受信装置３０に送信する。

【０２０４】

コンテンツデータ送信装置２０は、キー情報生成部２３のキー情報生成制御部２３ａにおいて新たにキー情報が選択された場合、コンテンツ暗号化部２２において新たに選択されたキー情報に基づいてコンテンツデータの暗号化を行い、その暗号化コンテンツデータを送信する際にコンテンツ送信データに新たに選択したキー情報に関する選択情報を格納し、コンテンツデータ受信装置３０に送信する。

【０２０５】

コンテンツデータ受信装置３０は、キー情報抽出部３３においてコンテンツ送信データに格納されている新たな選択情報に基づいてキー情報記憶部３３ａに記憶している複数のキー情報の中から前記選択情報に基づいて１つのキー情報を選択し、コンテンツ復号化部３４においてキー情報抽出部３３から得た新たなキー情報を用いて暗号化コンテンツデータを復号化する。

【０２０６】

このようにして、コンテンツデータ送信装置２０からコンテンツデータ受信装置３０にコンテンツデータを送信する。

【０２０７】

他の実施例のコンテンツデータ送受信システムにおいては、コンテンツデータの暗号化に用いるキー情報を複数生成し、複数のキー情報の中から選択した１つのキー情報を用いてコンテンツデータを暗号化してコンテンツデータ受信装置に送信することができるため、不正にキー情報、暗号化コンテンツデータを取得することが困難になり、暗号化コンテンツデータをキー情報を用いて復号してコンテンツデータの違法複製することを防止することができる。

【０２０８】

以上のように、本発明のコンテンツデータ送受信システムでは、コンテンツデータ送信装置とコンテンツデータ受信装置との間で、機器認証を行うための受信装置ＩＤ情報、暗号化コンテンツデータを復号するためのキー情報、暗号化したコンテンツデータを、複数のデータ列からなるそれぞれのデータに格納し、そのデータを複数の信号線を用いてコンテンツデータ受信装置に送信する。このため、コンテンツデータ送信装置が出力する受信装置ＩＤ情報、キー情報、暗号化コンテンツデータを単一の信号線から取得することができないため、不正に受信装置ＩＤ情報、キー情報、暗号化コンテンツデータを得て、暗号化コンテンツデータをキー情報を用いて復号してコンテンツデータの違法複製することを防止することができる。

【０２０９】

上述した実施例においては、コンテンツデータ送信装置からコンテンツデータ受信装置にデータを送信する信号線を６本の信号線（第１データ線～第６データ線）として説明したが、２本以上の多数の信号線であれはいずれの本数でもよい。

【０２１０】

コンテンツデータ送信装置からコンテンツデータ受信装置にデータを送信する信号線の本数を多いことにより、受信装置ＩＤ情報及びキー情報を分割する数が増えるため、信号線から受信装置ＩＤ情報及びキー情報を不正に取得しにくくすることができる。また、暗号化コンテンツデータも同様に取得しにくくすることができると共に、より多くのチャンネル数のオーディオデータを送信することも可能になる。

【０２１１】

また、上述した実施例では、コンテンツデータ送信装置からコンテンツデータ受信装置に接続確認データ、機器認証データ、キー送信データ、コンテンツ送信データを送信する際に、コンテンツデータ送信装置は、複数のデータ列を同時に送信しているが、複数のデータ列を時間差を設けて送信してもよい。すなわち、第１データ列を送信した後、予め定

めた時間経過後に第２データ列を送信し、同様に、第３データ列～第６データ列を時間差を設けて送信するようにしてもよい。

【０２１２】

このことにより、コンテンツデータ送信装置が送信したデータを同時刻に受信し、同時刻に受信したデータに格納されている情報の組み替えを行っただけでは、当該データに格納されている情報から正しい情報（例えば、受信装置ＩＤ情報、キー情報など）を取得することが困難になる。したがって、コンテンツデータ送信装置が出力する受信装置ＩＤ情報、キー情報、暗号化コンテンツデータを不正に取得し、そのデータを用いて暗号化コンテンツデータを復号してコンテンツデータを違法に複製することを防止することができる。

【図面の簡単な説明】

【０２１３】

【図１】本発明のコンテンツデータ送受信システムの一実施例を示す概略構成図。

【図２】本実施例のコンテンツデータ送受信システムにおける接続確認データ及び接続確認応答データのフォーマットを示す図。

【図３】本実施例のコンテンツデータ送受信システムにおける機器認証データ及び機器認証応答データのフォーマットを示す図。

【図４】本実施例のコンテンツデータ送受信システムにおけるキー情報送信データ及びキー情報受信データのフォーマットを示す図。

【図５】本実施例のコンテンツデータ送受信システムにおけるコンテンツ送信データ及びコンテンツ受信データのフォーマットを示す図。

【図６】本発明のコンテンツデータ送受信方法の一実施例を説明するための図。

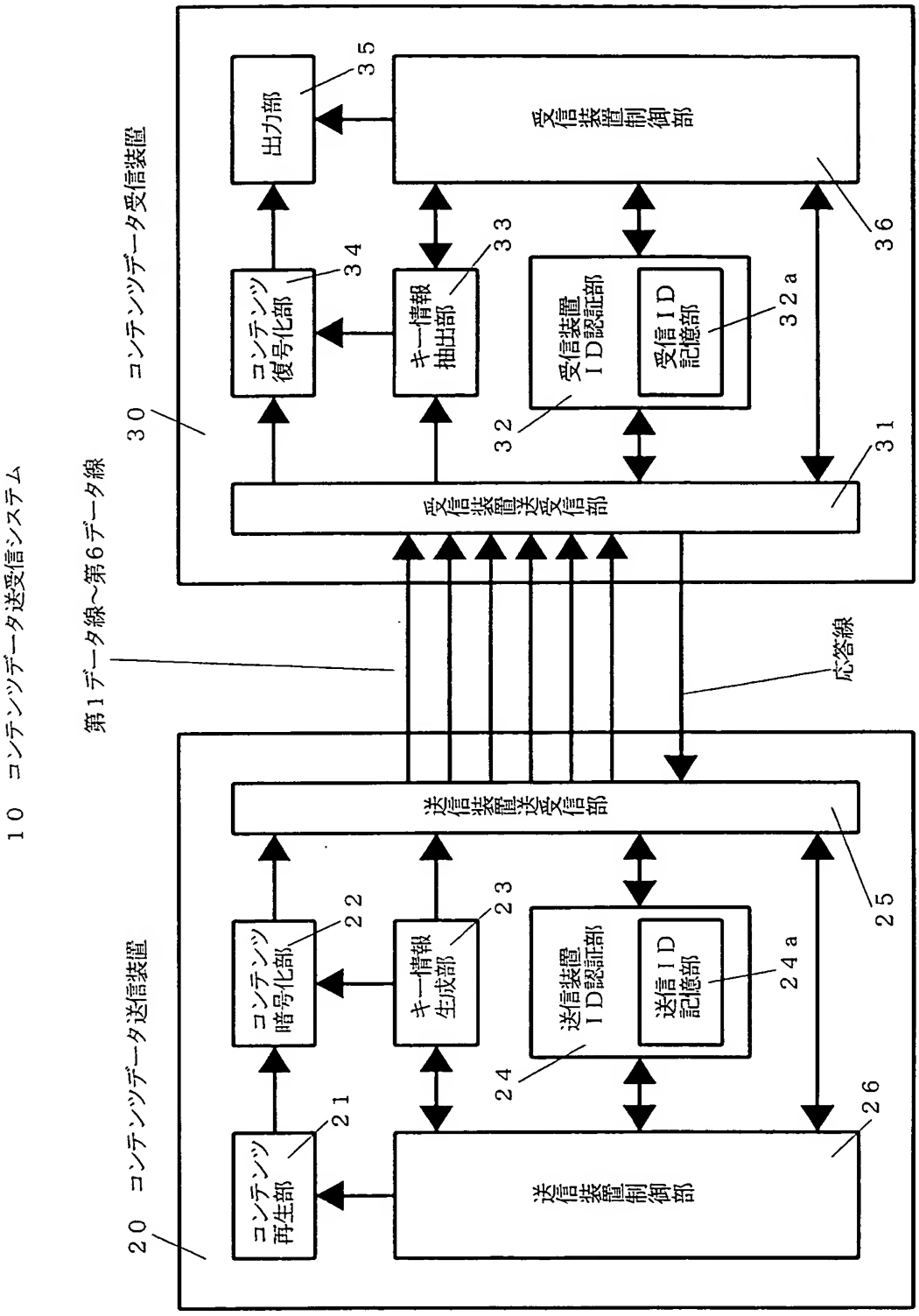
【図７】本発明のコンテンツデータ送受信システムの他の実施例を示す概略構成図。

【符号の説明】

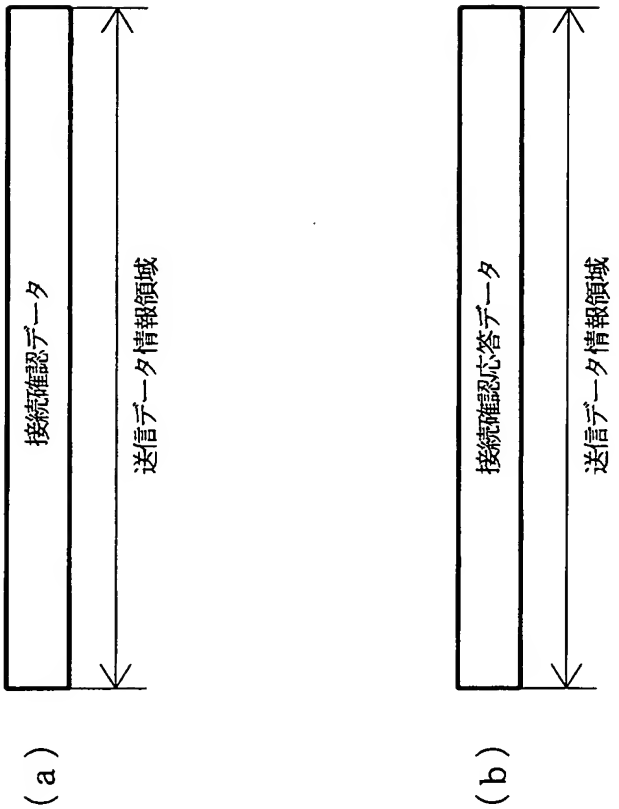
【０２１４】

１０・・・コンテンツデータ送受信システム、２０・・・コンテンツデータ送信装置、２１・・・コンテンツ再生部、２２・・・コンテンツ暗号化部、２３・・・キー情報生成部、２３ａ・・・キー情報生成制御部、２４・・・送信装置ＩＤ認証部、２４ａ・・・送信ＩＤ記憶部、２５・・・送信装置送受信部、２６・・・送信装置制御部、３０・・・コンテンツデータ受信装置、３１・・・受信装置送受信部、３２・・・受信装置ＩＤ認証部、３２ａ・・・受信ＩＤ記憶部、３３・・・キー情報抽出部、３３ａ・・・キー情報記憶部、３４・・・コンテンツ復号化部、３５・・・出力部、３６・・・受信装置制御部。

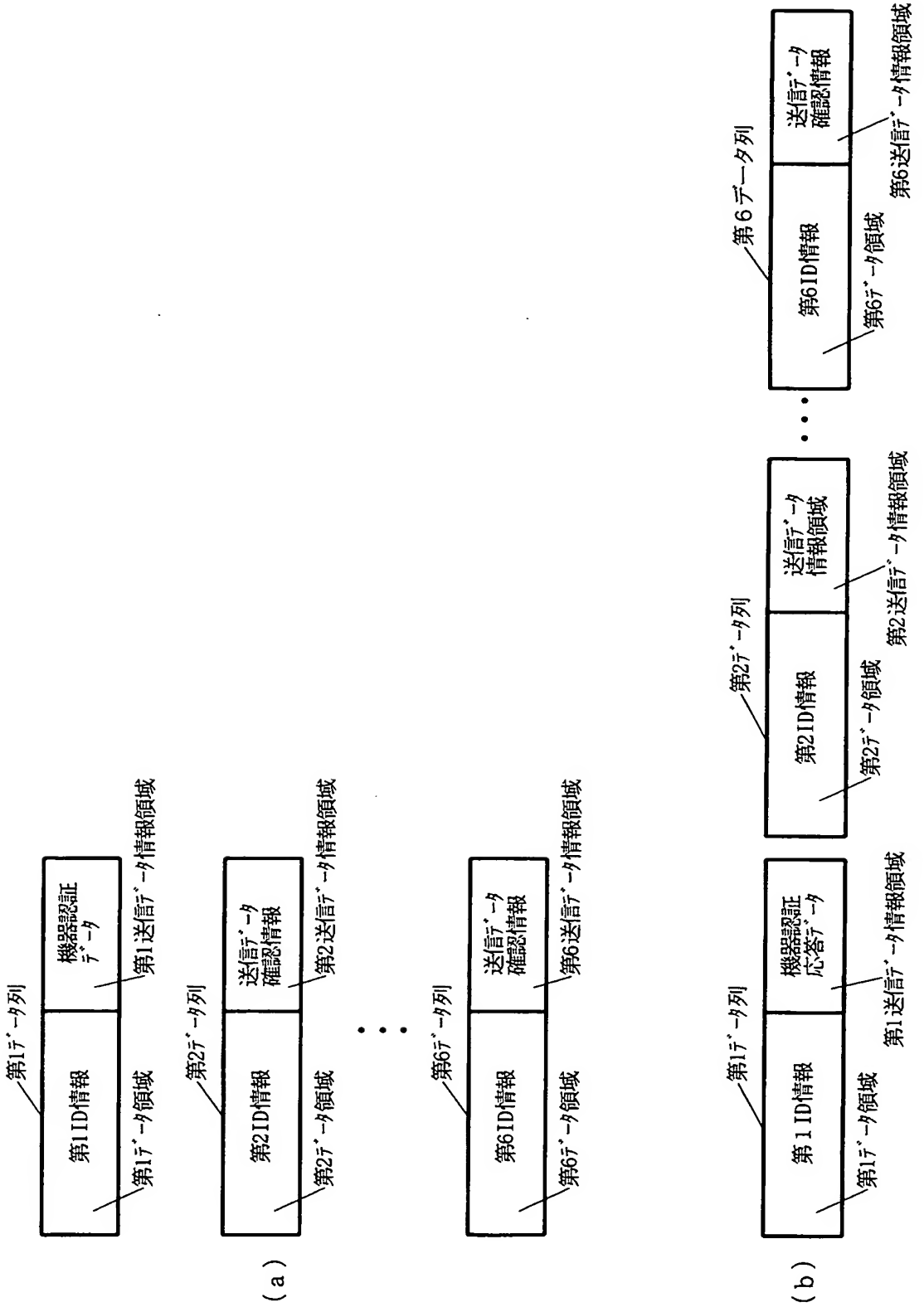
【書類名】図面
【図１】


１０　コンテンツデータ送受信システム
第１データ線～第６データ線
３０　コンテンツデータ受信装置
出力部
３５
受信装置制御部
３６
コンテンツ復号化部
３４
キー情報抽出部
３３
受信装置ＩＤ認証部
３２
受信ＩＤ記憶部
３２ａ
受信装置送受信部
３１
応答線
送信装置送受信部
２５
コンテンツ暗号化部
２２
キー情報生成部
２３
送信装置ＩＤ認証部
２４
送信ＩＤ記憶部
２４ａ
コンテンツ再生部
２１
送信装置制御部
２６
２０　コンテンツデータ送信装置

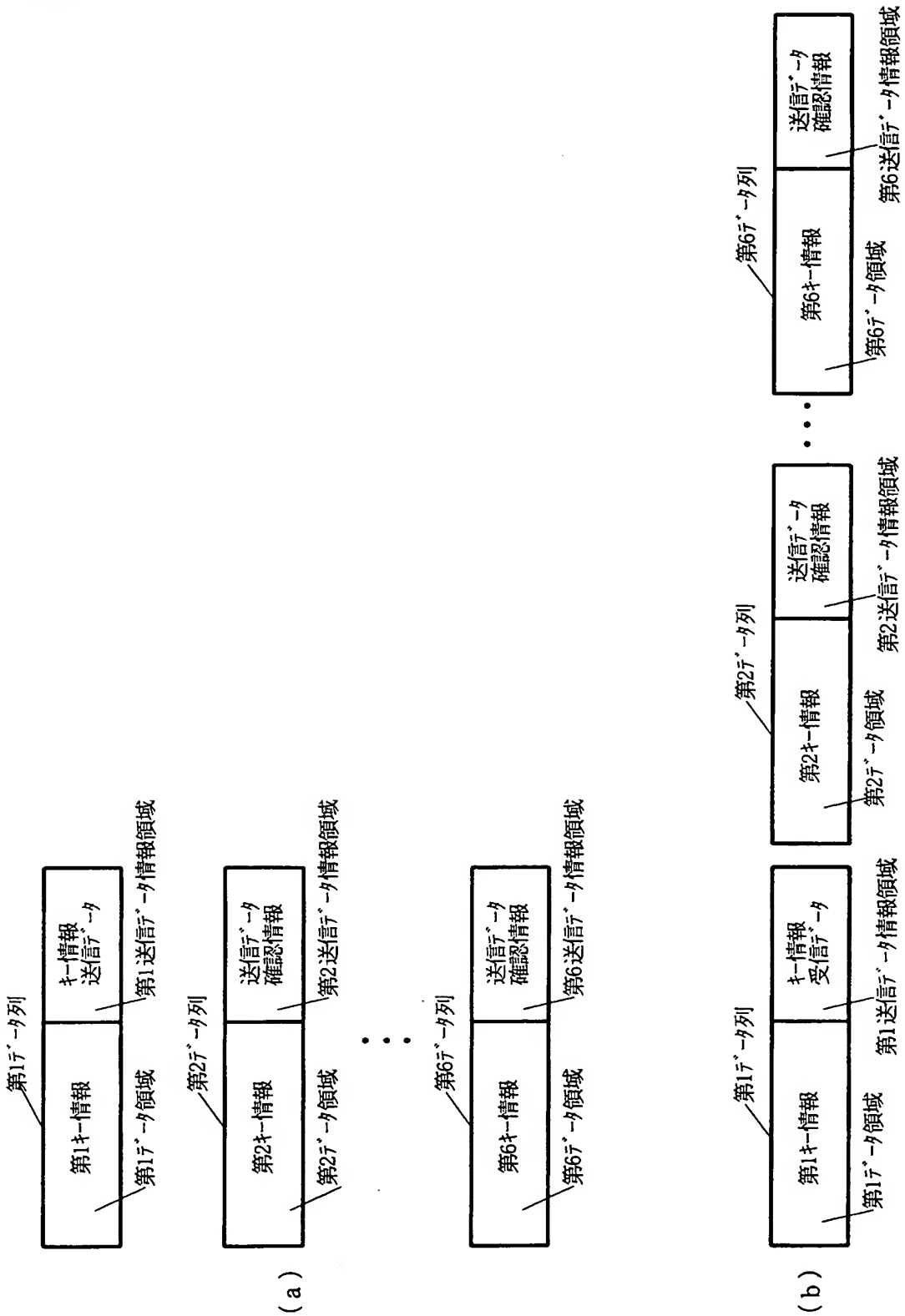
【図２】



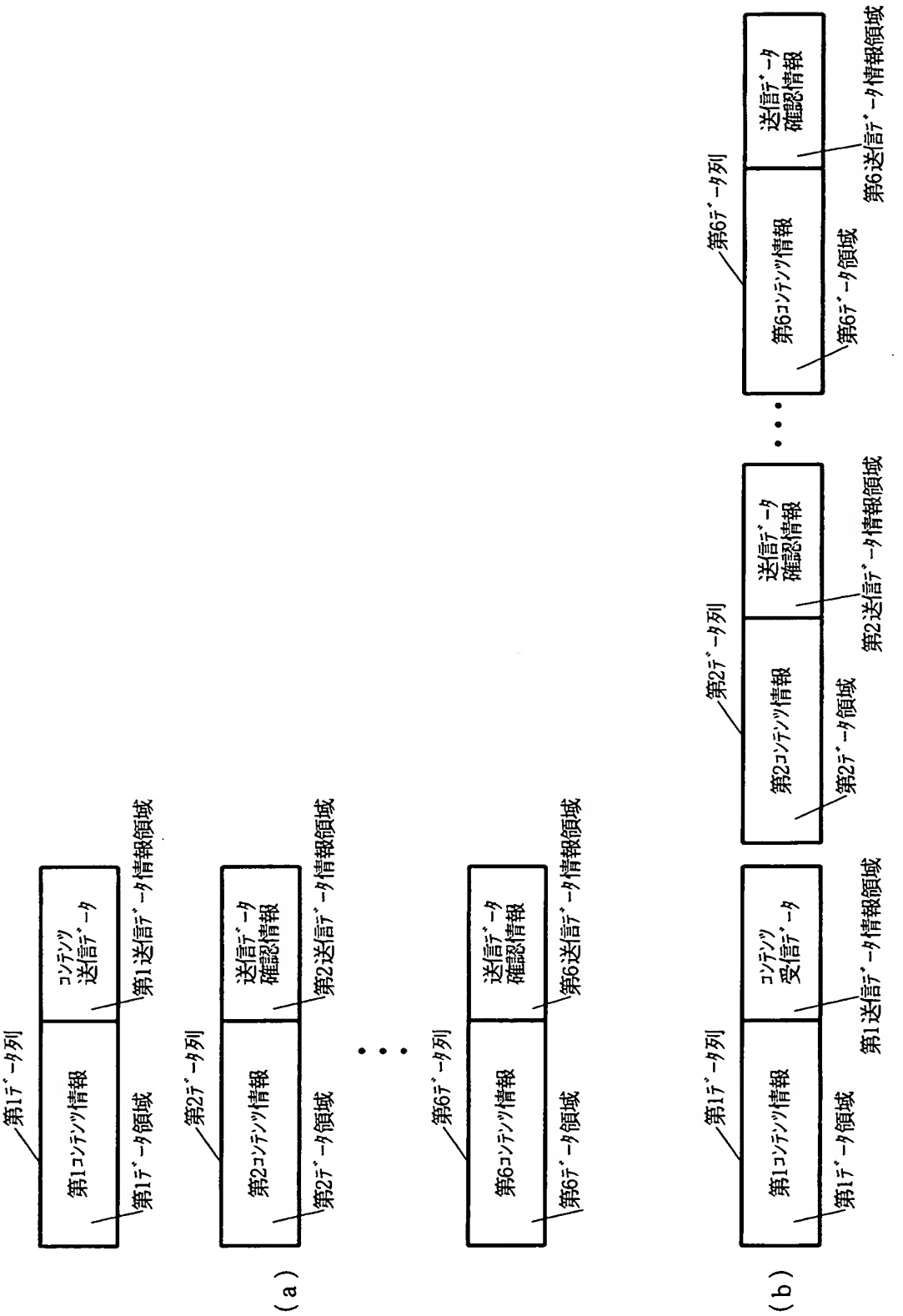
【図３】


(a)
第1ﾃﾞｰﾀ列
第1 ID情報
機器認証ﾃﾞｰﾀ
第1ﾃﾞｰﾀ領域
第1送信ﾃﾞｰﾀ情報領域
第2ﾃﾞｰﾀ列
第2ID情報
送信ﾃﾞｰﾀ確認情報
第2ﾃﾞｰﾀ領域
第2送信ﾃﾞｰﾀ情報領域
第6ﾃﾞｰﾀ列
第6ID情報
送信ﾃﾞｰﾀ確認情報
第6ﾃﾞｰﾀ領域
第6送信ﾃﾞｰﾀ情報領域
(b)
第1ﾃﾞｰﾀ列
第1 ID情報
機器認証応答ﾃﾞｰﾀ
第1ﾃﾞｰﾀ領域
第1送信ﾃﾞｰﾀ情報領域
第2ﾃﾞｰﾀ列
第2ID情報
送信ﾃﾞｰﾀ情報領域
第2ﾃﾞｰﾀ領域
第2送信ﾃﾞｰﾀ情報領域
第6ﾃﾞｰﾀ列
第6ID情報
送信ﾃﾞｰﾀ確認情報
第6ﾃﾞｰﾀ領域
第6送信ﾃﾞｰﾀ情報領域

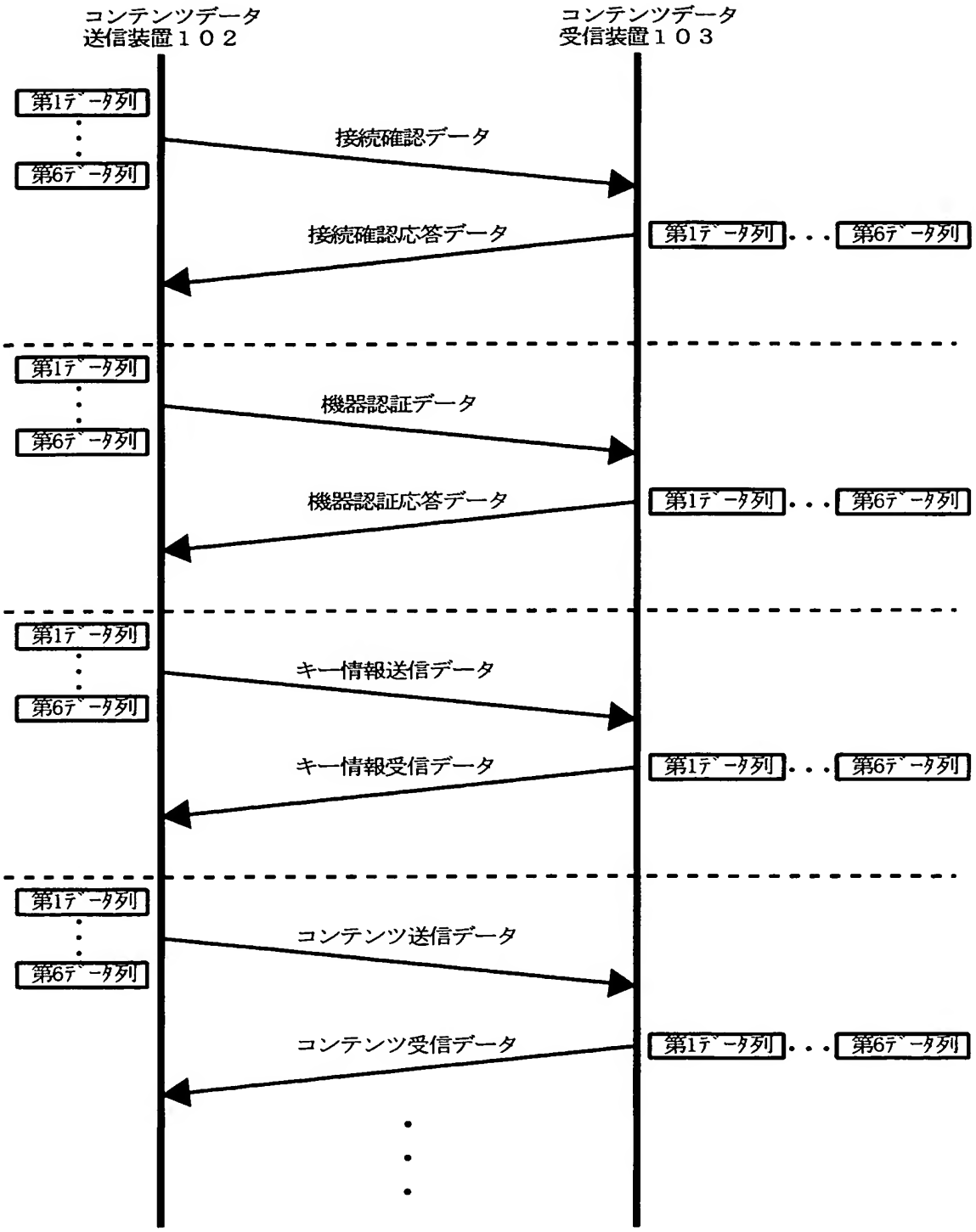
【図４】


第1データ列
第1キー情報
キー情報 送信データ
第1データ領域
第1送信データ情報領域
第2データ列
第2キー情報
送信データ 確認情報
第2データ領域
第2送信データ情報領域
第6データ列
第6キー情報
送信データ 確認情報
第6データ領域
第6送信データ情報領域
（a）
第1データ列
第1キー情報
キー情報 受信データ
第1データ領域
第1送信データ情報領域
第2データ列
第2キー情報
送信データ 確認情報
第2データ領域
第2送信データ情報領域
第6データ列
第6キー情報
送信データ 確認情報
第6データ領域
第6送信データ情報領域
（b）

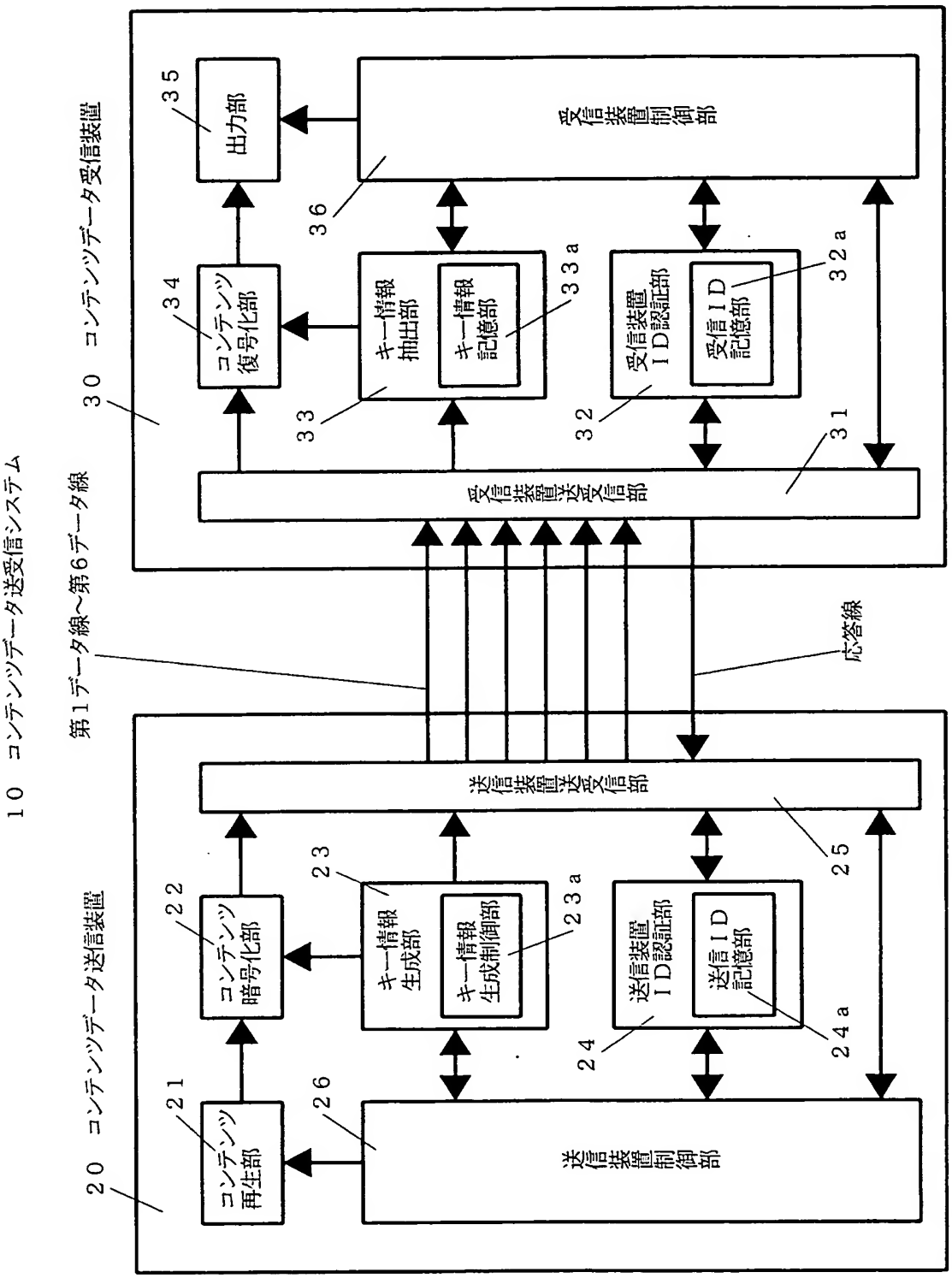
【図５】


(a)
第1データ列
第1コンテンツ情報
コンテンツ送信データ
第1データ領域
第1送信データ情報領域
第2データ列
第2コンテンツ情報
送信データ確認情報
第2データ領域
第2送信データ情報領域
第6データ列
第6コンテンツ情報
送信データ確認情報
第6データ領域
第6送信データ情報領域
(b)
第1データ列
第1コンテンツ情報
コンテンツ受信データ
第1データ領域
第1送信データ情報領域
第2データ列
第2コンテンツ情報
送信データ確認情報
第2データ領域
第2送信データ情報領域
第6データ列
第6コンテンツ情報
送信データ確認情報
第6データ領域
第6送信データ情報領域

【図６】


コンテンツデータ
送信装置１０２
コンテンツデータ
受信装置１０３
第1ﾃﾞｰﾀ列
第6ﾃﾞｰﾀ列
接続確認データ
接続確認応答データ
機器認証データ
機器認証応答データ
キー情報送信データ
キー情報受信データ
コンテンツ送信データ
コンテンツ受信データ

【図７】


１０　コンテンツデータ送受信システム
２０　コンテンツデータ送信装置
３０　コンテンツデータ受信装置
第１データ線～第６データ線
応答線
コンテンツ再生部
コンテンツ暗号化部
キー情報生成部
キー情報生成制御部
送信装置ＩＤ認証部
送信ＩＤ記憶部
送信装置制御部
送信装置送受信部
コンテンツ復号化部
キー情報抽出部
キー情報記憶部
受信装置ＩＤ認証部
受信ＩＤ記憶部
受信装置制御部
出力部
２１
２２
２３
２３ａ
２４
２４ａ
２５
２６
３１
３２
３２ａ
３３
３３ａ
３４
３５
３６

【書類名】要約書
【要約】
【課題】コンテンツデータ送受信システムでは、２台の装置を接続している単一の信号線を伝送しているデータから暗号解除情報を抽出し、暗号解除情報を用いて暗号化コンテンツデータを復号して元の高品質のコンテンツデータを得ることができるという問題がある。
【解決手段】コンテンツデータ送受信システムにおいて、コンテンツデータ送信装置は、コンテンツデータをキー情報を用いて暗号化し、キー情報を信号路を介してコンテンツデータ受信装置に送信した後にそのキー情報によって暗号化したコンテンツデータを複数の信号路を介してコンテンツデータ受信装置に送信する。コンテンツデータ受信装置は、コンテンツデータ送信装置から信号路を介して送信されたキー情報を取得し、コンテンツデータ送信装置から複数の信号路を介して送信された暗号化したコンテンツデータを受信し、キー情報を用いて前記暗号化したコンテンツデータを復号する。
【選択図】　図１

特願２００３－３１３８５２

出　願　人　履　歴　情　報

識別番号　　［３０１０６６００６］

１．変更年月日　　２００１年１０月　９日
［変更理由］　　新規登録
住　所　　東京都文京区湯島三丁目１６番１１号
氏　名　　株式会社デノン